Cisco Systems - Comprehensive Research

Overview

Cisco Systems is a global leader in networking and cybersecurity infrastructure, providing AI-powered technology solutions for modern enterprises. Their main value proposition is "AI Infrastructure, Secure Networking, and Software Solutions" with a focus on "Bringing the power of hyperscaler technology to the enterprise"[3].

Key Platforms Identified

- Cisco Hypershield: AI-native Security Architecture for Data Centers.
- Cisco Duo: Multi-factor authentication and identity security platform with 1B+ monthly authentications [5]
- Cisco Secure Endpoint: Cloud-native endpoint security with 85% reduction in remediation times [6]
- Webex Suite: The world's first unified, purpose-built suite for hybrid work

Main Navigation Sections

1. Products and Services
2. Solutions
3. Support
4. Learn
5. Partners
6. More (Resources)

Detailed Information Collection

Products and Services Section

Networking Products

- Access networking
- Data center and cloud networking
- Industrial IoT
- Internet, cloud, and endpoint visibility
- Network security
- Networking software
- Optics and transceivers
- Service provider networking
- Silicon
- Wide-area networking (WAN)

Cisco Networking Products

1. Access Networking

- Details: These products manage how end-users and devices (like computers, phones, and IoT sensors) connect to the network, whether wired or wirelessly.
- Key Features:
    - Switches: Enable local area network (LAN) connectivity, often with Power over Ethernet (PoE) for powering connected devices.
    - Wireless Access Points & Controllers: Provide Wi-Fi connectivity and centralized management of wireless networks.
    - Network Access Control (NAC): Enforces security policies on devices before they connect to the network.
- Benefits: Secure and reliable user and device connectivity, simplified deployment of network-powered devices, and granular control over network access.

2. Data Center and Cloud Networking

- Details: Designed for the demanding environments of data centers and for integrating with cloud services, focusing on high-speed data transfer and efficient resource utilization.
- Key Features:
    - High-Density, High-Speed Switches: Optimized for massive data flows within data centers.
    - Application Centric Infrastructure (ACI): A software-defined networking (SDN) solution that automates network provisioning and policy enforcement.
    - Cloud Interconnect Solutions: Facilitate secure and efficient connections between on-premises data centers and public cloud providers.
- Benefits: Enhanced application performance, automated network operations, agile cloud connectivity, and improved operational efficiency within data centers.

3. Industrial IoT (Internet of Things)

- Details: Networking solutions specifically built for operational technology (OT) environments, connecting sensors, machines, and control systems in harsh industrial settings.
- Key Features:
    - Ruggedized Routers and Switches: Designed to withstand extreme temperatures, vibrations, and other challenging industrial conditions.
    - IoT Gateways: Connect diverse IoT devices to the network and often perform data aggregation.
    - Industrial Wireless: Provides reliable wireless connectivity in tough environments.

- Benefits: Reliable and secure connectivity for industrial operations, enabling real-time data collection, remote monitoring, and automation in challenging environments.

4. Internet, Cloud, and Endpoint Visibility

- Details: Provides comprehensive insights into network traffic, application performance, and security posture across the entire IT infrastructure, including internet connections, cloud applications, and individual devices.
- Key Features:
    - Network Performance Monitoring (NPM): Tracks network health and identifies bottlenecks.
    - Application Performance Management (APM): Monitors application performance to ensure optimal user experience.
    - Endpoint Detection and Response (EDR): Detects and responds to malicious activity on user devices.
    - Cloud Visibility Tools: Provide insight into cloud usage and security.
- Benefits: Proactive identification of network and application issues, enhanced security posture through real-time threat detection, and improved operational efficiency by pinpointing performance bottlenecks.

5. Network Security

- Details: A broad portfolio of products aimed at protecting the network infrastructure from cyber threats, ensuring data integrity, confidentiality, and availability.
- Key Features:
    - Firewalls (Traditional & Next-Generation): Control network traffic based on security policies.
    - Intrusion Prevention Systems (IPS): Detect and prevent network intrusions.
    - Secure Access Service Edge (SASE): Converges networking and security functions in the cloud for secure access.
    - Threat Intelligence (Talos): Provides real-time threat insights to inform security defenses.
- Benefits: Robust defense against cyberattacks, protection of sensitive data, compliance with security regulations, and reduced risk of breaches.

6. Networking Software

- Details: The intelligent software layer that powers and manages Cisco's networking hardware, enabling advanced functionalities, automation, and simplified network operations.
- Key Features:

    - Cisco Catalyst Center (formerly DNA Center): Centralized management and automation for enterprise networks.
    - Cisco SD-WAN Manager: Orchestrates software-defined wide area networks for optimized traffic.
    - Cisco Meraki Platform: Cloud-managed networking for simplified deployment and management.
- Benefits: Automated network provisioning, simplified management, optimized network performance, and reduced operational complexity.

7. Optics and Transceivers

- Details: Essential components for high-speed data transmission over fiber optic cables, crucial for modern networks requiring high bandwidth.
- Key Features:
    - Transceivers: Convert electrical signals to optical signals and vice versa, allowing network devices to connect to fiber.
    - Various Form Factors: Support different speeds and distances for diverse network requirements.
- Benefits: Enable high-bandwidth, long-distance data transmission, support for rapidly growing data demands, and ensure reliable high-speed network backbone.

8. Service Provider Networking

- Details: Specialized hardware and software designed for the large-scale, complex networks operated by telecommunications and internet service providers.
- Key Features:
    - Carrier-Grade Routers and Switches: High-capacity, highly reliable devices built for massive traffic volumes.
    - 5G Infrastructure: Solutions for deploying next-generation mobile networks.
    - Optical Networking: High-capacity transport systems for long-haul and metropolitan networks.
- Benefits: Scalable and reliable delivery of telecommunications and internet services, support for rapidly evolving network technologies like 5G, and efficient management of massive network traffic.

9. Silicon

- Details: Refers to Cisco's investment in developing custom chip technology to optimize the performance, power efficiency, and unique features of its networking devices.
- Key Features:

    - Custom ASICs (Application-Specific Integrated Circuits): Chips designed specifically for networking functions.
    - Network Processors: Specialized processors optimized for handling network traffic.
- Benefits: Superior performance, lower power consumption, enhanced security capabilities, and the ability to integrate advanced features directly into hardware.

10. Wide-Area Networking (WAN)

- Details: Products that connect geographically separated locations, such as branch offices, remote workers, and cloud resources, enabling communication and data exchange across long distances.
- Key Features:
    - WAN Routers: Direct traffic between different networks.
    - SD-WAN (Software-Defined WAN): Uses software to manage and optimize WAN connections.
    - WAN Optimization: Techniques to improve application performance over WAN links.
- Benefits: Secure and efficient connectivity for distributed organizations, improved application performance for remote users, and cost-effective management of long-distance network connections.

Hardware Products

- Routers
- Switches
- Wireless

Cisco Hardware Products:

1. Routers

- Details: Routers are networking devices that connect multiple networks together, such as connecting a local area network (LAN) to the internet or connecting different branches of an organization.[2] They operate at the network layer (Layer 3) of the OSI model, using IP addresses to determine the best path for data packets to travel.
- Key Features (inferred from document context):
    - Network Interconnectivity: Facilitate communication between disparate networks.
    - Traffic Routing: Intelligently direct data packets along optimal paths.

    - WAN Connectivity: Support connections over wide-area networks (WANs) for remote offices and internet access.
    - Security Features: Often include built-in firewall capabilities and VPN support for secure communication.
    - Industrial Routers: (As mentioned in Industrial IoT) Ruggedized for harsh environments.
- Benefits: Enables global connectivity for organizations, optimizes data flow across complex networks, provides secure remote access, and ensures reliable communication between different network segments.

2. Switches

- Details: Switches are devices that connect multiple devices (like computers, servers, and printers) within the same local area network (LAN), allowing them to communicate efficiently. They learn the MAC addresses of connected devices to forward data only to the intended recipient, improving network performance compared to older hub technology.
- Key Features (inferred from document context):
    - LAN Connectivity: Provide multiple ports for connecting wired devices.
    - VLAN Support: Allow network segmentation for improved security and management.
    - Power over Ethernet (PoE): Can deliver power to connected devices (e.g., IP phones, wireless access points) over the Ethernet cable.
    - Data Center Switches: (As mentioned in Data Center and Cloud Networking) High-density, high-speed, and optimized for data center traffic.
    - Industrial Switches: (As mentioned in Industrial IoT) Ruggedized for industrial environments.
- Benefits: High-speed data transfer within a local network, improved network performance and security through intelligent traffic forwarding, simplified cabling and power for connected devices (with PoE), and scalability for growing networks.

3. Wireless

- Details: This category encompasses wireless access points (APs) and wireless LAN controllers (WLCs) that provide Wi-Fi connectivity. Access points broadcast wireless signals, allowing devices like laptops, smartphones, and tablets to connect to the network without physical cables. WLCs centrally manage multiple APs.
- Key Features (inferred from document context):
    - Wi-Fi Connectivity: Enable wireless network access for mobile and stationary devices.
    - Centralized Management: Wireless LAN controllers simplify the

configuration and monitoring of many access points.
    - Security Protocols: Support various encryption and authentication standards to secure wireless communication.
    - Industrial Wireless: (As mentioned in Industrial IoT) Optimized for reliability in harsh industrial settings.
- Benefits: Mobility and flexibility for users, simplified network deployment in areas where cabling is difficult, support for a high density of wireless devices, and secure wireless access.

Networking Services

- Services for enterprise networking
- View all networking products

Key Features of Enterprise Networking Services and Products:

1. Network Devices:
    - Routers: Connect different networks (e.g., LAN to WAN, or multiple LANs) and direct data traffic between them.
    - Switches: Promote efficient communication within a local area network (LAN) by forwarding data packets to the correct devices. They can be managed (offering advanced features like VLANs) or unmanaged (plug-and-play).
    - Wireless Access Points (APs): Extend wired networks to provide Wi-Fi connectivity, allowing devices to connect wirelessly.
    - Firewalls: Act as a security barrier, inspecting and controlling network traffic to block unauthorized access, malware, and other threats. This includes both perimeter firewalls (north-south traffic) and internal firewalls (east-west traffic).
    - Load Balancers: Distribute incoming network traffic across multiple servers or resources to optimize performance, prevent overload, and ensure high availability.
    - VPN Servers: Provide secure remote access by encrypting user connections over public networks like the internet.
    - Network Attached Storage (NAS): Dedicated storage devices on the network with their own IP addresses, offering centralized data storage and simplified file sharing.
2. Network Architectures and Technologies:
    - Local Area Networks (LANs): Connect devices within a limited geographical area, such as an office building or campus.

- Wide Area Networks (WANs): Connect geographically dispersed LANs, data centers, and remote offices, often utilizing technologies like SD-WAN.
- Cloud Networks: Leverage cloud services for hosting applications, data storage, and network infrastructure, enabling greater flexibility and scalability.
- Software-Defined Networking (SDN): Decouples the network's control plane from the physical hardware, allowing for centralized control, automation, and dynamic routing. This simplifies network management and provisioning.
- Edge Networking and Computing: Brings computation and data storage closer to data sources (e.g., IoT devices), enhancing efficiency and reducing latency.
- Network as a Service (NaaS): A consumption model where networking capabilities are delivered as a service, reducing the need for upfront hardware investments and on-premises IT teams.
- Hybrid Cloud and Multi-Cloud Connectivity: Seamlessly integrates on-premises infrastructure with various public and private cloud environments.

3. Security Features:

    - Zero-Trust Architectures: A security model that assumes no user or device is inherently trustworthy, requiring strict verification before granting access.
    - Intrusion Detection/Prevention Systems (IDS/IPS): Detect and prevent malicious activities on the network in real-time.
    - Encryption: Secures data during transmission and storage, protecting sensitive information from unauthorized access.
    - Authentication and Access Controls: Implement strong methods to restrict network access to authorized users only, often through role-based access control.
    - AI-driven Threat Detection: Uses artificial intelligence and machine learning to identify and respond to evolving cyber threats.
    - Security Information and Event Management (SIEM): Centralizes security logging and event data for analysis and threat detection.
    - Network Segmentation: Divides the network into smaller, isolated segments to limit the impact of a security breach.
4. Management and Automation:

    - Centralized Network Management: Provides a single pane of glass for monitoring, troubleshooting, and managing network devices and services across the entire infrastructure.
    - Network Automation: Automates repetitive tasks, simplifies

configurations, and accelerates service provisioning, reducing human error and improving efficiency.
    - AI Assistants and Machine Learning: Streamline IT operations, identify anomalies, and provide actionable insights for network optimization and troubleshooting.
    - Real-time Monitoring and Analytics: Provides visibility into network performance, bandwidth usage, and user experience, enabling proactive issue resolution.

Benefits of Robust Enterprise Networking Services:

1. Enhanced Productivity and Collaboration:
    - Seamless Communication: Facilitates instant communication through video conferencing, instant messaging, shared file storage, and project management platforms, regardless of physical location.
    - Efficient Resource Sharing: Enables centralized access to applications, data, and peripherals, reducing redundancy and ensuring all users have the necessary tools.
    - Streamlined Workflows: Optimized network performance leads to faster data transfers, quicker application access, and improved overall employee efficiency.
2. Improved Security and Data Protection:
    - Protection from Cyber Threats: Robust security measures like firewalls, intrusion detection, and encryption safeguard sensitive business data and infrastructure from unauthorized access, malware, and cyberattacks.
    - Regulatory Compliance: Helps organizations meet compliance mandates for data protection (e.g., GDPR, HIPAA).
    - Reduced Risk of Data Breaches: By controlling access, monitoring traffic, and enforcing security policies, the risk of data breaches is significantly minimized.
3. Scalability and Flexibility:
    - Adaptability to Growth: A well-designed network can easily accommodate new users, devices, applications, and locations without major disruptions.
    - Support for New Technologies: Provides a platform for smooth integration of emerging technologies like IoT, cloud computing, and private 5G.
    - Agile Deployment: Enables businesses to react quickly to evolving

market conditions and deploy new services faster.

4. Cost Savings and Efficiency:
    - Reduced Operational Costs: Centralizing resources, optimizing bandwidth usage, and automating tasks can significantly lower IT expenses.
    - Minimized Downtime: Proactive monitoring and faster issue resolution reduce costly network outages and their associated business impact.
    - Optimized Resource Allocation: Virtualization and cloud-based services enable businesses to maximize the efficient allocation of resources.
    - Predictable Costs (especially with NaaS): Shifting from capital expenditures to predictable operational expenditures can help with budgeting.
5. Better User Experience:
    - Fast and Reliable Access: Ensures employees and customers have consistent, high-performance access to applications, data, and services.
    - Reduced Latency: Optimizes network performance to minimize delays in data transfer, crucial for real-time applications and collaboration.
    - Seamless Mobility: Supports remote work, mobile devices, and flexible working arrangements, ensuring connectivity from anywhere.

Security Products

- AI-Powered Security Platform
    - Hypershield
    - AI Defense
    - Secure Access Service Edge (SASE)
    - Threat intelligence (Talos)

Security Products:

1. AI-Powered Security Platform

An AI-powered security platform leverages advanced artificial intelligence and machine learning (ML) techniques to enhance various aspects of cybersecurity, often integrating with existing security infrastructure.

- Automated Threat Detection and Identification:
    - Machine Learning (ML) & Deep Learning: Utilizes sophisticated algorithms to analyze vast amounts of security data in real-time, including network traffic, application usage, user behavior, and threat intelligence feeds. This enables the detection of known and unknown

(zero-day) threats, malware, and advanced persistent threats (APTs).
    - Behavioral Analytics (UEBA): Establishes baselines of "normal" behavior for users, devices, and networks. Any significant deviation from these baselines triggers alerts, helping to identify insider threats, compromised accounts, or novel attack techniques.
    - Anomaly Detection: Identifies unusual patterns or outliers in data that might indicate a security incident that traditional signature-based methods would miss. This is crucial for detecting sophisticated and rapidly evolving threats.
    - Contextual Analysis: Gathers and correlates data from various sources to provide a richer understanding of a threat, its potential impact, and its progression within the environment.
- Faster Incident Response and Remediation:
    - Automated Response Capabilities: Can initiate automated actions upon threat detection, such as isolating infected systems, blocking malicious IP addresses, quarantining files, or revoking access, significantly reducing the time to contain a breach.
    - Alert Prioritization and Triage: Reduces alert fatigue by analyzing and prioritizing security alerts based on their severity, context, and potential impact, allowing security teams to focus on the most critical threats.
    - Remediation Strategy Development: Can suggest viable remediation strategies or actions based on its analysis of detected behaviors and known vulnerabilities.
- Proactive Threat Prediction and Vulnerability Management:
    - Predictive Analytics: Learns from historical attack data and patterns to predict emerging threats and potential attack vectors, enabling organizations to proactively strengthen their defenses.
    - Vulnerability Identification and Prioritization: Helps to discover and prioritize vulnerabilities within systems and applications based on potential exploitability and impact.
    - Attack Surface Management: Provides insights into an organization's attack surface and can forecast potential risks.
- Operational Efficiency and Augmentation:
    - Automation of Routine Tasks: Automates repetitive and time-consuming tasks like log analysis, initial alert investigations, and vulnerability scanning, freeing up human security analysts for more complex and strategic work.
    - Reduced False Positives: AI algorithms are designed to improve the accuracy of threat identification, minimizing the alerts that turn out to be benign.

    - Resource Augmentation: Fills resource gaps for cybersecurity teams, especially smaller or less resourced ones, by providing continuous and consistent protection.
- Continuous Learning and Adaptation:
    - Adaptive Models: Systems continuously learn from new data, including new attack techniques and threat patterns, ensuring that defenses remain effective against evolving threats.
    - Model Retraining: Algorithms are regularly updated and refined based on new intelligence and performance metrics.
- Integration with Existing Security Infrastructure:
    - API-Driven Integration: Designed to seamlessly integrate with Security Information and Event Management (SIEM) systems, Security Orchestration, Automation, and Response (SOAR) platforms,[1] firewalls, endpoint detection and response (EDR) solutions, and threat intelligence feeds.

2. Hypershield

Hypershield is an advanced, AI-native security architecture designed to provide pervasive and autonomous security across modern data centers, cloud environments, and distributed enterprise networks. It shifts security enforcement closer to the workloads.

- AI-Native and Autonomous Architecture:
    - Self-Managing Operations: Architected from the ground up to operate autonomously and with predictive capabilities. Once initial trust is established, it can manage security operations independently.
    - Autonomous Rule Generation: The system can autonomously generate, test, deploy, and manage its own security rules and policies.
- Hyper-Distributed Enforcement:
    - Security at the Edge/Workload: Integrates security enforcement points directly into various components, including:
        - Servers: Security agents operate on the workload, interfacing with processes and the operating system kernel via extended Berkeley Packet Filter (eBPF) technology (for Linux environments).
        - Data Processing Units (DPUs): Leverages specialized hardware (DPUs) to offload security processing from general-purpose CPUs, embedding high-performance security directly into network and

server hardware.
        - Network Ports/Switches: Transforms every network port into a high-efficiency point for security enforcement, extending protection to the network fabric itself.
        - Virtual Machines/Containers: Includes enforcement points that operate within VMs or containers, strategically placed close to the workload for more effective protection.
    - Pervasive Coverage: Ensures security measures can be implemented precisely where they are needed, covering every application service in data centers, Kubernetes clusters in public clouds, and every container and virtual machine.
- Application-Centric Security:
    - Deep Workload Visibility: Provides granular visibility into workload actions, monitoring network connections, file and system calls, and kernel functions. It alerts on anomalous activities specific to application processes.
    - Behavioral Analysis of Application Processes: Classifies and responds to suspicious or malicious activity by analyzing known application behaviors and process graphs.
- Automated Micro-segmentation:
    - Continuous Learning and Adaptation: Automatically learns and adapts segmentation policies, dynamically applying highly specific controls to isolate compromised segments and prevent the lateral movement of threats within the network.
    - Regex Filtering: Supports granular segmentation controls, including regular expression filtering for tailored security.
- Distributed Exploit Protection:
    - Near-Instantaneous Protection: Delivers protection against application vulnerabilities and exploits within minutes, often without requiring traditional software patches.
    - Self-Qualifying Updates: Automates software and policy upgrades by testing them in a "digital twin" environment using live traffic and policies. This allows for safe, zero-downtime updates and ensures that new rules will not break existing applications or services.
    - Dual Data-Plane Approach: Uses a dual data plane to safely test changes on live traffic without disrupting operations.
- Zero Trust Security Model:
    - Adopts a strict Zero Trust framework, verifying the legitimacy of every device and user accessing the network, and granting least-privilege

access based on strict identity verification and real-time threat analysis.

- Unified Cloud Management:
    - Centralized Policy Management: Provides a single, centralized management console (e.g., Cisco Defense Orchestrator - CDO) for organizing and managing all security policies.
    - Dynamic Policy Adaptation: Policies are compiled and distributed to appropriate enforcement points, dynamically adapting to workloads moving between on-premises environments, public clouds, or different servers.
- Cloud-Native Foundation:
    - Built on open-source eBPF technology, which allows for deep visibility and control within the Linux kernel, critical for securing and interconnecting cloud-native applications.

3. AI Defense (General Concept)

"AI Defense" typically refers to the broad application of Artificial Intelligence and Machine Learning technologies to enhance cybersecurity defenses, proactively detect threats, and automate responses. It encompasses many features also found in an "AI-Powered Security Platform," emphasizing the defensive use cases of AI in cybersecurity.

- Automated Threat Detection:
    - Real-time Analysis: Utilizes AI/ML to analyze massive volumes of real-time data (network traffic, user activity, application logs, endpoint data) to identify subtle patterns and indicators of compromise that human analysts might miss.
    - Signature-less Detection: Excels at identifying novel and polymorphic malware, zero-day attacks, and sophisticated threats that don't have known signatures.
    - Multi-Domain Analysis: Can correlate data across different domains (network, endpoint, cloud, email, identity) to build a holistic view of potential threats.
- Predictive Analysis:
    - Threat Forecasting: Leverages historical attack data and threat intelligence to anticipate future attack trends, potential attack vectors, and likely targets.
    - Vulnerability Prediction: Can predict which vulnerabilities attackers are most likely to exploit based on their tactics, techniques, and procedures

(TTPs).

- Behavioral Analytics:
    - User and Entity Behavior Analytics (UEBA): Builds profiles of normal behavior for users, devices, and applications. AI identifies anomalies or deviations from these baselines that could indicate compromised credentials, insider threats, or sophisticated attacks.
- Automated Response and Remediation:
    - Rapid Containment: AI systems can automatically trigger responses, such as isolating infected systems, blocking malicious IP addresses, or modifying firewall rules, to contain threats within seconds of detection.
    - Automated Remediation Workflows: Can execute predefined playbooks or suggest remediation steps to security analysts.
- Reduced False Positives and Alert Fatigue:
    - Intelligent Prioritization: AI algorithms analyze the context and severity of alerts to prioritize the most critical threats, significantly reducing the volume of false positives and allowing security teams to focus on actionable intelligence.
- Continuous Learning and Adaptation:
    - Adaptive Threat Models: Continuously learns from new threat data, observed attack patterns, and security incidents to refine its models and improve detection accuracy over time.
    - Self-Improvement: The AI models can evolve to counter new and evolving attack techniques.
- Operational Efficiency:
    - Automation of Repetitive Tasks: Automates mundane security tasks, such as log review, initial investigations, and data correlation, which frees up human analysts to handle more complex strategic tasks.
- Enhanced Situational Awareness:
    - Rich Contextual Insights: Provides security teams with deep insights and context around threats, including the "who, what, when, and how" of an attack.

4. Secure Access Service Edge (SASE)

SASE (pronounced "sassy") is a cloud-native architecture that converges networking (SD-WAN) and a comprehensive suite of security functions (Security Service Edge -

SSE) into a single, cloud-delivered service. It provides secure and flexible access to applications and data for users anywhere, on any device.

- Converged Networking and Security:
    - Single Unified Service: Combines Wide Area Network (WAN) optimization (via SD-WAN) with a full stack of security services into a single, integrated, cloud-native platform.
    - Eliminates Point Solutions: Replaces the need for multiple disparate security appliances and point solutions, reducing complexity and operational overhead.
- Key Security Service Edge (SSE) Components:
    - Secure Web Gateway (SWG): Provides comprehensive security for web traffic, including URL filtering, content inspection, malware protection, and application control.
    - Firewall as a Service (FWaaS): Delivers cloud-native firewall capabilities with advanced features like intrusion prevention, deep packet inspection, and access blocking for all traffic, not just web.
    - Cloud Access Security Broker (CASB): Extends security policies to cloud applications, providing visibility, data loss prevention (DLP), threat protection, and compliance assurance for SaaS and IaaS environments.
    - Zero Trust Network Access (ZTNA): Replaces traditional VPNs with a "never trust, always verify" model. It grants least-privilege, identity-based access to specific applications and resources, continuously verifying user, device, and context before and during access.
    - Data Loss Prevention (DLP): Monitors, detects, and prevents sensitive data from being exfiltrated from the organization's network, cloud applications, or endpoints.
    - Remote Browser Isolation (RBI): (Often included) Executes web Browse sessions in an isolated environment, protecting users from malicious web content.
- Software-Defined Wide Area Network (SD-WAN) Capabilities:
    - Optimized Routing: Dynamically routes traffic over the most efficient path (internet, MPLS, cellular) to ensure optimal application performance and user experience.
    - Global Connectivity: Leverages a global network of Points of Presence (PoPs) to provide low-latency, high-performance connectivity for users worldwide.
    - Cloud Acceleration: Prioritizes and optimizes traffic to cloud-based applications (SaaS, IaaS).

- Cloud-Native Architecture:
    - Globally Distributed PoPs: Services are delivered from a distributed network of cloud-based Points of Presence, ensuring proximity to users and applications for reduced latency.
    - Elastic and Scalable: Designed to scale dynamically to accommodate growing user bases, devices, and traffic volumes without requiring hardware upgrades.
    - Resilient and Self-Healing: Cloud-native design provides inherent resilience and automatic recovery from infrastructure disruptions.
- Identity-Based Access and Contextual Security:
    - User and Device Identity: Access policies are based on verified user identities, device posture, location, time of day, and application sensitivity, rather than just IP addresses.
    - Continuous Evaluation: Security posture is continuously assessed throughout a session, with access dynamically adjusted based on changing risk factors.
- Centralized Management and Unified Policy:
    - Single Pane of Glass: Provides a unified console for managing and monitoring all networking and security functions, simplifying policy enforcement across the entire enterprise.
    - Consistent Policy Enforcement: Ensures consistent security policies are applied to all users, devices, and locations, whether they are in the office, at home, or on the road.
- Enhanced Visibility and Control:
    - Comprehensive Visibility: Offers end-to-end visibility into all network traffic, user activities, and application usage across hybrid and multi-cloud environments.
    - Application-Layer Control: Classifies and controls traffic at the application layer (Layer 7), providing granular control over application usage.

5. Threat Intelligence (Talos)

Talos is the threat intelligence and research group at Cisco. It focuses on identifying, analyzing, and mitigating cyber threats on a global scale, providing actionable intelligence that protects Cisco's products, customers, and the broader internet community.

- Global Telemetry and Data Collection:

    - Vast Sensor Network: Collects an immense volume of real-time security data from Cisco's global network, products, and services (e.g., firewall logs, email telemetry, endpoint data, web traffic, intrusion prevention systems, honeypots). This includes billions of daily security events and millions of new malware samples analyzed constantly.
    - Diverse Data Sources: Gathers information from various sources like honeypots, spam traps, malware submissions, and direct observation of attack campaigns.
- Advanced Threat Research and Analysis:
    - Malware Analysis: Conducts in-depth analysis of malware, ransomware, exploits, and other malicious software to understand their tactics, techniques, and procedures (TTPs).
    - Vulnerability Research and Disclosure: Proactively identifies and researches security vulnerabilities (including zero-days) in software, hardware, and operating systems. Talos practices responsible disclosure, working with vendors to ensure patches are developed and released.
    - Campaign Tracking: Monitors and analyzes ongoing cyberattack campaigns, identifying threat actors, their motivations, and their methods.
    - Reverse Engineering: Conducts reverse engineering of malicious code to understand its functionality and develop countermeasures.
- Real-time Protection Updates:
    - Rapid Dissemination: Quickly converts raw threat data into actionable intelligence and automatically disseminates it to Cisco's security products (e.g., Secure Firewall, Umbrella, Secure Endpoint, Secure Email, NGIPS). This provides immediate protection against newly identified threats.
    - Automated Rule Generation: Develops and deploys signatures, rules, and behavioral indicators for various security controls (e.g., Snort rules, ClamAV definitions).
- Incident Response (Talos IR):
    - Proactive and Reactive Services: Offers services to help organizations prepare for, respond to, and recover from security breaches and cyber incidents. This includes forensic analysis, containment, eradication, and recovery planning.
- Community and Collaboration:
    - Open-Source Contributions: Actively contributes to and maintains popular open-source security projects like Snort (an open-source

intrusion prevention system) and ClamAV (an open-source antivirus engine).
    - Information Sharing: Collaborates with other cybersecurity organizations, government agencies, law enforcement, and industry groups to share threat intelligence and best practices, strengthening the global cybersecurity ecosystem.
- Strategic and Predictive Intelligence:
    - Contextual Intelligence: Provides rich context around threats, including the origin, intent, and potential impact, going beyond just technical indicators.
    - Adversary Profiling: Develops profiles of threat actors and groups, understanding their capabilities, targets, and typical operational methods.
    - Strategic Insights: Offers broader strategic insights into the evolving cyber threat landscape, helping organizations understand risks and develop long-term security strategies.

- Security Suites
    - Breach Protection Suite
    - Cloud Protection Suite
    - User Protection Suite

Security Suites: Detailed Key Features

1. Breach Protection Suite

A Breach Protection Suite focuses on enabling an organization to quickly detect, contain, and remediate security breaches across the most prominent attack vectors (email, endpoints, network, cloud). It's built for rapid response and minimizing the impact of a successful attack.

- Extended Detection and Response (XDR):
    - Unified Visibility: Collects and correlates telemetry data from various security layers (endpoints, email, network, cloud, identity, applications) to provide a holistic view of an attack.
    - Automated Investigation: Uses AI and machine learning to automatically analyze security events, piece together attack narratives, and identify the scope and impact of a threat.
    - Threat Prioritization: Reduces alert fatigue by using contextualization and analytics to prioritize the most critical threats, helping security operations center (SOC) teams focus their efforts.

    - Proactive Threat Hunting: Enables security analysts to actively search for hidden threats and sophisticated attack campaigns across the integrated security telemetry.
    - Automated Remediation: Can trigger automated actions to contain and respond to threats, such as isolating compromised endpoints, blocking malicious files, or removing phishing emails.
    - Root Cause Analysis: Helps identify how a threat entered the environment and what assets were affected.
- Endpoint Detection and Response (EDR) / Secure Endpoint:
    - Advanced Malware Protection (AMP): Detects, blocks, and retrospectively analyzes advanced malware, ransomware, and fileless attacks on endpoints (laptops, desktops, servers).
    - Real-time Threat Detection: Continuously monitors endpoint activity (process execution, file changes, network connections) for suspicious behaviors.
    - Threat Hunting Capabilities: Allows security teams to query endpoint data for signs of compromise.
    - Vulnerability Management: Helps identify and manage vulnerabilities on endpoint devices.
    - Rapid Containment and Remediation: Provides capabilities to isolate compromised endpoints and remove malicious artifacts.
- Secure Email Threat Defense:
    - Anti-Phishing and Anti-Spoofing: Detects and blocks sophisticated phishing attacks, business email compromise (BEC), and spoofed emails that attempt to trick users.
    - Malware and Ransomware Protection: Scans email attachments and links for malicious content, including known and zero-day malware.
    - Spam Filtering: Filters out unwanted spam email, reducing noise and potential attack vectors.
    - Data Loss Prevention (DLP) for Email: Prevents sensitive information from being sent out of the organization via email.
    - Attachment Sandboxing: Detonates suspicious email attachments in a secure, isolated environment to analyze their behavior before they reach user inboxes.
- Network Analytics / Network Detection and Response (NDR):
    - Network Visibility: Provides deep insights into network traffic patterns, baselines normal behavior, and detects anomalies that could indicate a breach or malicious activity (e.g., command-and-control communication, lateral movement).
    - Flow Data Analysis (e.g., NetFlow/IPFIX): Analyzes network flow data for security insights without requiring full packet capture.
    - Behavioral Anomaly Detection: Uses machine learning to identify deviations from normal network activity, such as unusual data transfers, unauthorized access attempts, or new device connections.
    - Threat Hunting on the Network: Enables security analysts to search for specific indicators of compromise or attack patterns within network data.
- Secure Malware Analytics (Sandboxing):

    - Dynamic Malware Analysis: Executes unknown or suspicious files in a virtual, isolated environment (sandbox) to observe their real-time behavior without risking the production network.
    - Threat Intelligence Generation: Extracts indicators of compromise (IoCs) and threat intelligence from the analysis, which can then be shared with other security tools for broader protection.
    - Threat Scoring: Provides a risk score for analyzed files, helping to prioritize investigations.

2. Cloud Protection Suite

A Cloud Protection Suite is designed to secure an organization's applications, data, and infrastructure across hybrid and multi-cloud environments. It addresses the unique security challenges of cloud adoption, offering end-to-end visibility and protection.

- Cloud Workload Protection (CWP) / Secure Workload:
    - Micro-segmentation: Provides granular network segmentation at the workload level (VMs, containers) to isolate applications and prevent lateral movement of threats within cloud environments.
    - Application Dependency Mapping: Maps application components and their communication flows to understand and enforce appropriate security policies.
    - Vulnerability Management for Workloads: Identifies and prioritizes vulnerabilities within cloud workloads and container images.
    - Runtime Protection: Monitors and protects running workloads from attacks, ensuring only authorized processes and communications occur.
    - Compliance for Workloads: Helps maintain compliance with regulatory standards by enforcing security policies across workloads.
- Cloud Security Posture Management (CSPM):
    - Continuous Configuration Monitoring: Automatically monitors cloud infrastructure (IaaS, PaaS, SaaS) for misconfigurations, policy violations, and security risks.
    - Compliance Benchmarking: Assesses cloud environments against industry standards (e.g., CIS Benchmarks, NIST, GDPR, HIPAA) and regulatory frameworks.
    - Risk Prioritization: Identifies and prioritizes cloud security risks based on severity and potential impact.
    - Automated Remediation: Can automatically remediate common misconfigurations or provide detailed steps for manual remediation.
- Cloud Native Application Protection Platform (CNAPP) / Multicloud Defense:
    - Full Lifecycle Protection: Provides security across the entire cloud-native application lifecycle, from development (Infrastructure-as-Code scanning, container image scanning) to runtime.
    - Unified Cloud Security: Integrates CSPM, CWP, Cloud Infrastructure Entitlement Management (CIEM), and other cloud security capabilities into a single platform for comprehensive protection across multiple cloud providers.
    - API Security: Secures APIs used by cloud-native applications from abuse and attacks.

    - Container and Kubernetes Security: Provides specialized security for containerized applications, including image scanning, runtime protection, and Kubernetes environment security.
- Cloud Access Security Broker (CASB):
    - Visibility into Cloud App Usage: Discovers and monitors sanctioned and unsanctioned cloud applications (shadow IT) used within the organization.
    - Data Loss Prevention (DLP) for Cloud: Enforces policies to prevent sensitive data from being uploaded to unauthorized cloud apps or shared improperly.
    - Threat Protection for Cloud Apps: Detects and prevents malware and other threats within cloud applications.
    - Compliance Enforcement: Helps ensure compliance with data residency and other regulatory requirements for cloud data.
- Cloud Firewall / Cloud Network Firewall:
    - Traffic Filtering and Inspection: Provides advanced firewall capabilities in the cloud, including deep packet inspection, intrusion prevention, and access control for traffic moving to, from, and within cloud environments.
    - Segmentation in the Cloud: Enables network segmentation within cloud virtual networks to limit lateral movement.
    - Elastic Scalability: Scales automatically to handle varying traffic loads in cloud environments.
- Vulnerability Management for Cloud:
    - Automated Scanning: Continuously scans cloud resources (VMs, containers, functions) for known vulnerabilities.
    - Risk-based Prioritization: Prioritizes vulnerabilities based on exploitability, impact, and asset criticality.
    - Integration with DevOps: Integrates security checks into the CI/CD pipeline to identify vulnerabilities early in the development lifecycle.

3. User Protection Suite

A User Protection Suite focuses on securing the end-user, their devices, and their access to applications and data, regardless of location. It is crucial for supporting remote and hybrid work models and implementing a Zero Trust security approach.

- Secure Access / Zero Trust Network Access (ZTNA):
    - Identity-Centric Access: Grants access based on verified user identity and device posture, not just network location. "Never trust, always verify."
    - Least-Privilege Access: Provides granular access to specific applications or resources, rather than broad network access (like a traditional VPN).
    - Continuous Verification: Continuously evaluates trust and context throughout a user's session, dynamically adjusting access if risk factors change.
    - Device Posture Check: Verifies the security hygiene of the accessing device (e.g., up-to-date OS, antivirus

installed, disk encryption).

- Multi-Factor Authentication (MFA) / Adaptive MFA (e.g., Cisco Duo):
    - Strong Identity Verification: Requires users to provide two or more verification factors (e.g., password + phone push, biometrics, hardware token) to confirm their identity.
    - Contextual Authentication: Adapts authentication requirements based on risk factors such as location, device, network, and access history.
    - User Experience (UX) Focused: Aims to provide strong security with minimal friction for the user.
- Endpoint Protection Platform (EPP) / Secure Endpoint:
    - Antivirus/Anti-Malware: Real-time protection against viruses, worms, Trojans, ransomware, and other malicious software.
    - Exploit Prevention: Blocks exploit attempts against software vulnerabilities.
    - Host-based Firewall: Controls network connections on the endpoint.
    - Device Control: Manages access to peripheral devices (USB drives, etc.).
- Secure Web Gateway (SWG):
    - Web Content Filtering: Blocks access to malicious, inappropriate, or non-compliant websites.
    - Threat Protection: Scans web traffic (HTTP/HTTPS) for malware, phishing attempts, and other web-borne threats.
    - URL Filtering and Category Blocking: Allows organizations to control which types of websites users can access.
    - SSL/TLS Inspection: Decrypts and inspects encrypted web traffic for hidden threats.
- Secure Email Gateway / Email Threat Defense:
    - Phishing and Spam Protection: Filters out unwanted emails, identifies and blocks phishing attempts, and prevents social engineering attacks.
    - Malware in Email: Scans email attachments and links for malicious code.
    - Impersonation Protection: Detects attempts to impersonate legitimate users or organizations.
- Remote Browser Isolation (RBI):
    - Client-Side Protection: Executes web Browse sessions in a remote, isolated container, sending only a safe, rendered image of the webpage to the user's browser.
    - Eliminates Web-borne Threats: Prevents malicious code from ever reaching the user's device, protecting against drive-by downloads, zero-day exploits, and advanced phishing.
- Data Loss Prevention (DLP) for Endpoints and Cloud:
    - Sensitive Data Monitoring: Monitors user activities and data transfers to identify and prevent the unauthorized exfiltration of sensitive information from endpoints or cloud applications.
    - Policy Enforcement: Enforces policies to control how sensitive data can be used, stored, and shared.

- Security Awareness Training:
    - User Education: Provides training programs to educate users about common cyber threats (phishing, social engineering) and best security practices.
    - Simulated Phishing Attacks: Conducts simulated phishing campaigns to test user susceptibility and reinforce training.

- Featured Security Products
    - Cisco Duo
    - Email Threat Defense
    - Firewall
    - Identity Services Engine (ISE)
    - Secure Access (SSE)
    - Secure Endpoint

Featured Security Products:

1. Cisco Duo

Cisco Duo is a leading multi-factor authentication (MFA) and access security platform that focuses on verifying user identities and device health before granting access to applications and data, embodying a core principle of Zero Trust security.

- Multi-Factor Authentication (MFA):
    - Flexible Authentication Methods: Supports a wide range of MFA options including Duo Push (push notifications to mobile devices), FIDO2/WebAuthn (phishing-resistant security keys), biometrics (fingerprint, facial recognition), hardware tokens, SMS passcodes, and phone call authentication.
    - User-Friendly Experience: Designed for ease of use, making strong authentication less intrusive for end-users, which increases adoption rates.
    - Phishing Resistance: Offers phishing-resistant MFA methods (like FIDO2 and Verified Duo Push) to protect against advanced phishing attacks and MFA fatigue.
- Device Trust and Visibility:
    - Trusted Endpoints Verification: Checks if a device is registered, managed, or compliant with security policies (e.g., up-to-date OS, enabled firewall, antivirus installed) before allowing access. Can block access from untrusted or unmanaged devices.
    - Device Health and Posture Checks: Gathers detailed information about the security posture of accessing devices, providing visibility into device health and potential vulnerabilities.
- Adaptive and Risk-Based Authentication:
    - Contextual Policies: Dynamically adjusts authentication requirements based on contextual factors such as user

location, device type, network, application being accessed, and historical behavior. Higher risk attempts trigger stronger authentication.
    - Risk-Based Analytics: Utilizes machine learning (e.g., Duo Trust Monitor) to assess the risk of a login attempt in real-time, detecting anomalies and potential ongoing attacks.
- Single Sign-On (SSO):
    - Streamlined Access: Allows users to log in once with Duo and securely access multiple cloud and on-premises applications without re-authenticating, improving user experience and productivity.
- Passwordless Authentication:
    - Reduced Password Reliance: Enables users to securely log in without a password using Duo Mobile push notifications or FIDO2 authenticators, simplifying logins and reducing password-related support costs.
- Zero Trust Security Support:
    - "Never Trust, Always Verify": Aligns with Zero Trust principles by continuously verifying the identity of users and the health of devices before granting and maintaining access to applications and data.
- Centralized Management and Reporting:
    - Admin Dashboard: Provides a unified dashboard for administrators to manage users, devices, applications, and security policies.
    - Comprehensive Reporting: Offers detailed reports on authentication attempts, device health, and policy enforcement, providing insights into security posture.
- Integration Capabilities:
    - Extensive Application Integrations: Integrates seamlessly with a wide range of cloud and on-premises applications, VPNs, and identity providers via standard protocols (e.g., SAML, RADIUS).
    - API Support: Provides Admin APIs for automated and scalable administrative management and integration with other security tools.

2. Email Threat Defense

Email Threat Defense solutions provide multi-layered protection against a wide spectrum of email-borne threats, which remain a primary vector for cyberattacks like phishing, ransomware, and business email compromise (BEC).

- Advanced Malware and Ransomware Protection:
    - Signature-based Detection: Identifies and blocks known malware using regularly updated threat intelligence.
    - Heuristic and Behavioral Analysis: Detects new and evolving malware by analyzing suspicious behaviors or characteristics, even if no signature exists.
    - Attachment Sandboxing/Detonation: Executes suspicious email attachments in a secure, isolated virtual

environment to observe their behavior in real-time without risking the production network. Malicious files are identified and blocked before reaching user inboxes.

- Anti-Phishing and Anti-Spoofing:
    - Link Protection (URL Rewriting/Click-Time Protection): Rewrites URLs in emails to direct clicks through a security gateway for real-time analysis at the time of click, blocking access to malicious or suspicious sites even if the link was initially benign.
    - Spoofing and Impersonation Detection: Detects attempts to spoof legitimate domains or impersonate executives (BEC attacks) using various techniques, including DMARC, DKIM, SPF checks, and AI-driven behavioral analysis of sender reputation and email content.
    - Credential Phishing Detection: Specifically identifies and blocks emails designed to steal login credentials, often by analyzing suspicious login page URLs or forms.
- Spam Filtering:
    - High Catch Rates: Effectively filters out unwanted spam emails, reducing inbox clutter and the risk of users accidentally clicking on malicious links or attachments within spam.
- Data Loss Prevention (DLP) for Email:
    - Outbound Content Inspection: Scans outgoing emails for sensitive information (e.g., credit card numbers, PII, intellectual property) to prevent unauthorized data exfiltration.
    - Policy Enforcement: Enforces policies to block, encrypt, or quarantine emails containing sensitive data.
- Post-Delivery Remediation (e.g., Office 365 Clawback):
    - Automated Email Removal: Allows security teams to automatically search for and remove malicious emails from user inboxes even after they have been delivered, crucial for mitigating fast-moving threats.
- Threat Intelligence Integration:
    - Real-time Updates: Leverages global threat intelligence (like Cisco Talos) to stay updated on the latest threats, attack campaigns, and indicators of compromise (IoCs).
- Internal Email Protection:
    - East-West Traffic Inspection: Scans internal email communications to detect and prevent threats originating from compromised internal accounts or insider threats.
- Reporting and Analytics:
    - Visibility into Email Threats: Provides dashboards and reports that offer insights into email threat trends, blocked attacks, and user-reported issues.

3. Firewall (Next-Generation Firewall - NGFW)

Modern firewalls, particularly Next-Generation Firewalls (NGFWs), go far beyond basic packet filtering to provide comprehensive, multi-layered network security.

- Stateful Packet Inspection (SPI):
    - Session Tracking: Monitors the state of active network connections and allows only legitimate traffic to pass through, blocking unsolicited packets.
- Application Visibility and Control (AVC):
    - Application-Layer Awareness (Layer 7): Identifies and controls applications running on the network, regardless of port or protocol. Can block, allow, or limit bandwidth for specific applications (e.g., block social media, prioritize VoIP).
- Intrusion Prevention System (IPS):
    - Signature-based Detection: Identifies and blocks known attack patterns and exploits.
    - Anomaly-based Detection: Detects suspicious network behavior that may indicate an unknown attack.
    - Threat Intelligence Integration: Leverages real-time threat intelligence to update IPS signatures and detection capabilities.
- Advanced Malware Protection (AMP) / Sandbox Integration:
    - File Reputation and Analysis: Checks the reputation of files traversing the network.
    - Dynamic Malware Analysis (Sandboxing): Detonates suspicious files in an isolated virtual environment to observe their behavior and identify malicious intent before they reach endpoints.
- URL Filtering and Web Content Filtering:
    - Category-based Blocking: Blocks access to malicious, inappropriate, or non-compliant websites based on predefined categories.
    - Reputation-based Filtering: Blocks access to sites with known bad reputations.
- VPN Capabilities:
    - Site-to-Site VPN: Creates secure, encrypted tunnels between geographically dispersed networks (e.g., branch offices to HQ).
    - Remote Access VPN (SSL VPN, IPsec VPN): Provides secure, encrypted access for individual remote users to the corporate network (often integrating with endpoint VPN clients like Cisco AnyConnect).
- Encrypted Traffic Analysis (ETA) / SSL/TLS Inspection:
    - Visibility into Encrypted Traffic: Can decrypt and inspect SSL/TLS encrypted traffic for hidden threats, then re-encrypt it before forwarding. Some NGFWs can detect malware within encrypted traffic *without* full

decryption.

- Identity Awareness / User-ID Integration:
    - User and Group-based Policies: Enforces security policies based on user identities and group memberships (e.g., Active Directory integration) rather than just IP addresses.
- Centralized Management:
    - Unified Management Console (e.g., Cisco Firepower Management Center - FMC): Provides a single pane of glass for configuring policies, monitoring events, and managing multiple firewall devices across the network.
- High Availability and Scalability:
    - Clustering and Failover: Supports clustering multiple firewall devices for redundancy and increased throughput, ensuring continuous operation.

4. Identity Services Engine (ISE)

Cisco Identity Services Engine (ISE) is a powerful Network Access Control (NAC) solution that enables organizations to enforce security policies, manage network access, and ensure endpoint compliance based on user identity, device type, and security posture. It's a cornerstone of Zero Trust architectures.

- Network Access Control (NAC):
    - Authentication (AuthN): Verifies user and device identities using various methods (e.g., 802.1X, MAC address authentication, web authentication) against identity sources (e.g., Active Directory, LDAP, internal databases).
    - Authorization (AuthZ): Grants granular network access based on context – who the user is, what device they are using, their location, time of day, and the security posture of their device.
    - Accounting (AAA): Logs user and device activity for auditing and compliance purposes.
- Device Profiling and Classification:
    - Automatic Device Identification: Automatically identifies and classifies devices connecting to the network (e.g., IoT devices, printers, IP phones, BYOD devices) based on various attributes (MAC OUI, DHCP, HTTP user-agent, NMAP scans).
    - Endpoint Context: Builds a rich context about each connecting endpoint, including its type, operating system, and security status.
- Posture Assessment (Endpoint Compliance):
    - Health Checks: Assesses the security posture of endpoints (laptops, mobile devices) before and during access. Checks for presence of antivirus, firewall status, OS patches, unauthorized applications, etc.
    - Remediation: Can redirect non-compliant devices to a remediation portal to install missing software or updates before granting network access.

    - Persistent and Non-Persistent Agents: Supports continuous monitoring with persistent agents (e.g., Cisco AnyConnect) or temporary checks with non-persistent agents.
- Secure Network Segmentation:
    - Policy-based Segmentation: Dynamically assigns users and devices to specific network segments (VLANs, Security Group Tags - SGTs) based on their identity and compliance status, limiting lateral movement of threats.
    - Micro-segmentation: Can extend segmentation down to the application or workload level when integrated with other solutions (e.g., Cisco Secure Workload).
- Guest Access Management:
    - Customizable Guest Portals: Provides secure and seamless self-service portals for guest user registration and access, often with sponsor approval workflows.
- Threat Containment and Integration:
    - Rapid Threat Containment: Integrates with firewalls, IPS, and other security tools (via Cisco pxGrid) to automatically quarantine or restrict access for compromised devices in real-time upon threat detection.
    - Threat Intelligence Sharing: Shares contextual information (user identity, device details) with other security solutions to enhance threat detection and response.
- BYOD (Bring Your Own Device) Support:
    - Secure Onboarding: Facilitates secure self-service onboarding of personal devices while ensuring they comply with organizational security policies.
    - MDM Integration: Integrates with Mobile Device Management (MDM) systems for enhanced control over mobile devices.
- Centralized Policy Management:
    - Single Policy Enforcement Point: Consolidates access policy creation and management across wired, wireless, and VPN networks.

5. Secure Access (SSE - Security Service Edge)

Cisco Secure Access is Cisco's Security Service Edge (SSE) solution, which provides a unified, cloud-delivered platform for securing access to the web, cloud services, and private applications for a distributed workforce. It's the security component of a SASE architecture.

- Converged Cloud Security Functions:
    - Secure Web Gateway (SWG): Protects users from web-borne threats, enforces web content filtering, and provides URL filtering and SSL/TLS inspection for all web traffic.
    - Zero Trust Network Access (ZTNA): Replaces traditional VPNs, providing identity-based, least-privilege access

to private applications and resources. It ensures that only authorized users and healthy devices can connect to specific applications.
    - Cloud Access Security Broker (CASB): Provides visibility and control over cloud application usage (SaaS and IaaS), enforcing DLP, threat protection, and compliance policies for cloud data.
    - Firewall as a Service (FWaaS): Delivers cloud-native firewall capabilities for inspecting and controlling all internet-bound and cloud-bound traffic.
- Cloud-Native and Globally Distributed Architecture:
    - Global Points of Presence (PoPs): Delivered from a globally distributed network of cloud data centers, ensuring low-latency access and consistent security enforcement for users anywhere.
    - Scalability and Resilience: Inherently elastic and designed to scale to meet the demands of a growing, distributed workforce.
- Identity-Based Security:
    - User and Device Context: Enforces security policies based on validated user identities, device posture, and other contextual factors, central to a Zero Trust model.
    - Continuous Trust Verification: Continuously evaluates trust throughout a user's session.
- Data Loss Prevention (DLP):
    - Multi-mode DLP: Detects and prevents the exfiltration of sensitive data across web, cloud applications, and private applications.
- Threat Protection and Intelligence:
    - Advanced Malware Protection (AMP): Detects and blocks malware, ransomware, and other advanced threats.
    - Threat Intelligence Integration (Talos): Leverages Cisco Talos's global threat intelligence for real-time threat detection and prevention.
    - DNS-layer Security: Blocks malicious domains at the DNS layer, preventing connections to command-and-control servers, phishing sites, and other malicious destinations.
- Remote Browser Isolation (RBI):
    - Web Content Sandboxing: Isolates risky web content by executing it in a remote, disposable container, rendering a safe, interactive stream to the user's browser, thus eliminating browser-borne threats.
- Unified Management and Simplified Operations:
    - Single Console: Provides a centralized, cloud-managed console for simplified deployment, management, and policy enforcement across all SSE functions.
    - Single Client: Often uses a unified agent (e.g., Cisco Secure Client) on endpoints to provide consistent security and access.
- User Experience Insights:

    - Performance Monitoring: Includes capabilities to monitor application performance and availability (e.g., integration with ThousandEyes) to ensure a good user experience and aid in troubleshooting.

6. Secure Endpoint (formerly Cisco AMP for Endpoints)

Cisco Secure Endpoint is a cloud-managed Endpoint Detection and Response (EDR) solution that provides comprehensive protection against advanced threats across various operating systems. It focuses on prevention, detection, response, and continuous monitoring of endpoint activity.

- Advanced Malware Prevention (AMP):
    - File Reputation and Analysis: Leverages a global cloud-based threat intelligence database to determine the reputation of files and block known malware.
    - Machine Learning (ML) and Behavioral Analysis: Detects new and polymorphic malware, fileless attacks, and sophisticated threats by analyzing file behavior and process execution in real-time.
    - Exploit Prevention: Protects against attempts to exploit vulnerabilities in applications and operating systems.
    - Antivirus Capabilities: Provides traditional signature-based antivirus protection.
- Endpoint Detection and Response (EDR):
    - Continuous Monitoring: Continuously monitors all endpoint activity (file changes, process execution, network connections, memory activity) to detect suspicious behaviors and indicators of compromise (IoCs).
    - Visibility into Endpoint Activity: Provides a detailed history of endpoint events, allowing security analysts to investigate incidents thoroughly.
    - Automated Root Cause Analysis: Automatically maps out the entire attack chain, from initial compromise to remediation, providing a clear understanding of the threat's scope and impact.
- Threat Hunting Capabilities:
    - Orbital Advanced Search: Allows security analysts to perform real-time, custom queries across all endpoints to proactively hunt for hidden threats, identify suspicious artifacts, and validate security posture.
    - Threat Intelligence Integration (Talos): Leverages Cisco Talos's extensive threat intelligence to enrich endpoint data and provide context for detected threats.
- Automated Response and Remediation:
    - Rapid Containment: Provides capabilities to quickly isolate compromised endpoints from the network to prevent lateral movement of threats.
    - Automated Remediation: Can automatically remove malicious files, terminate malicious processes, and restore systems to a pre-infection state.
    - Quarantine: Automatically quarantines suspicious files.
- Vulnerability Management:

    - Risk-Based Vulnerability Detection: Identifies vulnerabilities on endpoints and prioritizes them based on risk levels and potential impact, helping IT teams focus remediation efforts.
- Cross-Platform Protection:
    - OS Support: Provides consistent protection across various operating systems, including Windows, macOS, Linux, and often supports mobile platforms.
- Cloud-Native Architecture:
    - Scalability: Cloud-based management and analytics scale to protect large numbers of endpoints.
    - Global Coverage: Delivers protection regardless of where the endpoint is located.
- Integration with XDR and Security Ecosystem:
    - XDR Integration: Feeds endpoint telemetry into broader Extended Detection and Response (XDR) platforms (like Cisco SecureX) to provide a unified view of threats across multiple security domains (endpoint, network, email, cloud).
    - API-Driven Integration: Integrates with other security tools and IT systems for enhanced automation and orchestration.

- Network Security Categories
    - Hybrid Mesh Firewall
    - Industrial security
    - Network security
    - User and device security

Network Security Categories

1. Hybrid Mesh Firewall

A Hybrid Mesh Firewall refers to an advanced architectural approach to firewall deployment that combines the strengths of various firewall forms (physical appliances, virtual firewalls, cloud-native firewalls) to create a unified, pervasive security fabric across an organization's entire distributed infrastructure. This includes on-premises data centers, public cloud environments, hybrid cloud setups, and increasingly, the network edge and industrial environments.

- Distributed Enforcement Points:
    - Physical Firewalls (NGFWs): Traditional hardware firewalls deployed in data centers, campus perimeters, and branch offices, providing high throughput and deep packet inspection.
    - Virtual Firewalls (vFirewalls): Software-based firewalls deployed within virtualized environments (VMware, Hyper-V) or private clouds, offering

flexibility and scalability for internal network segmentation.
    - Cloud-Native Firewalls (FWaaS): Firewall capabilities delivered as a service from the cloud, securing traffic to and from public cloud resources (IaaS, PaaS, SaaS) and often acting as a secure access point for remote users.
    - Micro-segmentation Firewalls (Workload Protection): Granular, software-based firewalls embedded directly on individual workloads (VMs, containers, bare-metal servers) to enforce segment-of-one security, preventing lateral movement within highly dynamic environments.
    - Edge/IoT Firewalls: Compact, specialized firewalls designed for industrial (OT) or Internet of Things (IoT) environments, offering basic yet robust security in resource-constrained settings.
- Centralized Policy Management:
    - Unified Management Plane: A single, consolidated management console or platform (e.g., Cisco Secure Firewall Management Center) to define, deploy, and enforce security policies across all distributed firewall instances, regardless of their location or form factor.
    - Policy Orchestration and Automation: Automates the translation and distribution of high-level security policies into specific rules for different firewall types and environments.
- Consistent Security Posture:
    - Uniform Policy Enforcement: Ensures that security policies are applied consistently across all parts of the hybrid network, reducing security gaps and ensuring compliance.
    - Policy Synchronization: Automatically synchronizes policy changes across the mesh to maintain consistency and reduce manual configuration errors.
- Threat Intelligence Sharing:
    - Integrated Threat Feeds: All firewall instances in the mesh leverage shared, real-time threat intelligence (e.g., Cisco Talos) to detect and block the latest threats, ensuring rapid protection against new attacks.
    - Automated Updates: Security updates, signatures, and rules are automatically distributed to all relevant firewall components.
- Visibility and Analytics:
    - Holistic Traffic Visibility: Provides a comprehensive view of network traffic flowing across the entire hybrid environment, including encrypted traffic.
    - Centralized Logging and Reporting: Aggregates logs and security events

from all firewall components for unified monitoring, analysis, and compliance reporting.
    - Behavioral Analytics: Uses machine learning to detect anomalous behavior within the mesh that might indicate a sophisticated attack.
- Dynamic Scalability and Agility:
    - Elasticity: Firewall resources can scale up or down dynamically in cloud and virtual environments to meet changing traffic demands.
    - Hybrid Cloud Integration: Seamlessly integrates security for workloads moving between on-premises data centers and various public cloud providers.
- Zero Trust Enforcement:
    - Micro-segmentation at Scale: Facilitates the implementation of Zero Trust by enforcing granular access controls and "least privilege" across the entire mesh, limiting lateral movement of threats.
    - Identity-based Policies: Integrates with identity management systems to enforce policies based on user and device identity.

2. Industrial Security (Operational Technology - OT Security)

Industrial Security focuses on protecting Operational Technology (OT) and Industrial Control Systems (ICS) which manage and control physical processes in sectors like manufacturing, energy, utilities, transportation, and critical infrastructure. These environments have unique characteristics and vulnerabilities compared to traditional IT networks.

- Asset Discovery and Inventory (Passive):
    - Deep Packet Inspection (DPI) for OT Protocols: Passive monitoring of industrial network traffic to discover and identify OT assets (PLCs, RTUs, HMIs, sensors, actuators), their firmware versions, and their communication patterns without disrupting operations.
    - Vulnerability Mapping: Maps discovered assets to known vulnerabilities in OT/ICS databases.
- Network Visibility and Anomaly Detection:
    - Baseline Creation: Establishes baselines of normal OT network communication patterns and process variables.
    - Anomaly Detection: Identifies deviations from these baselines, such as unauthorized device connections, unusual commands, changes in program logic, or abnormal traffic flows, which could indicate a cyberattack or operational issue.

    - Protocol-Specific Analysis: Understands and analyzes proprietary industrial protocols (e.g., Modbus/TCP, EtherNet/IP, DNP3, OPC UA) for security analysis.
- OT Network Segmentation and Enforcement:
    - Zone Segmentation: Enforces logical or physical segmentation of OT networks into zones (e.g., Purdue Model) to limit the spread of malware and contain breaches.
    - Unidirectional Gateways: (Often used in conjunction) Devices that allow data flow in only one direction (e.g., from OT to IT) to provide an air gap for critical systems.
    - Policy Enforcement: Applies security policies to control communication between different OT segments and between OT and IT networks, ensuring only authorized traffic passes.
- Threat Detection and Prevention for OT:
    - Industrial IPS/IDS: Intrusion detection/prevention capabilities tailored to recognize and block threats specific to OT protocols and attack patterns.
    - Malware Detection for OT: Detects malware designed to target industrial control systems (e.g., Stuxnet, Triton).
- Secure Remote Access for OT:
    - Strict Access Controls: Provides secure, identity-verified, and tightly controlled remote access for vendors, maintenance personnel, and internal staff to OT systems, often requiring MFA and session recording.
    - Jump Boxes/Bastion Hosts: Utilizes hardened intermediary systems to control and monitor access.
- Vulnerability Management for OT:
    - Non-intrusive Scanning: Employs passive or low-impact scanning techniques to identify vulnerabilities in OT assets without risking system downtime or disruption.
    - Patch Management Strategies: Provides guidance and tools for managing patches in highly sensitive OT environments, often requiring scheduled downtime.
- Centralized Management and Integration (OT-IT Convergence):
    - Unified Visibility: Provides a single pane of glass for OT security, integrating with broader enterprise security operations (SIEM, SOAR) to correlate IT and OT alerts.
    - Risk Assessment and Reporting: Generates reports specific to OT security posture and compliance.

- Cyber-Physical Systems (CPS) Protection:
    - Integrates security for devices that bridge the digital and physical worlds.

3. Network Security (General Enterprise Focus)

Network security encompasses the hardware and software solutions that protect an organization's network infrastructure and data from unauthorized access, misuse, modification, or destruction. It's a broad category covering various layers of defense.

- Firewalling (Next-Generation Firewalls - NGFW):
    - Deep Packet Inspection (DPI): Examines the contents of network packets beyond headers to identify and control applications and detect threats.
    - Application Visibility and Control (AVC): Identifies and controls applications running on the network regardless of port.
    - Intrusion Prevention System (IPS): Actively blocks known and suspicious network attack patterns.
    - URL Filtering/Web Content Filtering: Blocks access to malicious or inappropriate websites.
    - VPN (Virtual Private Network): Secure, encrypted tunnels for remote access (remote access VPN) and site-to-site connectivity.
- Network Segmentation:
    - VLANs (Virtual LANs): Logical segmentation of a network into smaller broadcast domains.
    - Micro-segmentation: Granular segmentation to isolate individual workloads or applications, limiting lateral movement.
    - Security Zones: Dividing the network into logical zones (e.g., DMZ, internal, server farms) with specific security policies governing traffic between them.
- Network Access Control (NAC):
    - Authentication, Authorization, and Accounting (AAA): Controls who (user identity), what (device type), and how (policy-based access) can connect to the network.
    - Device Posture Assessment: Checks the security compliance of devices connecting to the network (e.g., antivirus status, patch level).
    - Guest Access Management: Securely manages access for visitors and personal devices.
- Network Detection and Response (NDR):

    - Traffic Monitoring and Analysis: Continuously monitors network traffic (flow data, packet capture) for anomalies, suspicious patterns, and indicators of compromise (IoCs).
    - Behavioral Anomaly Detection: Uses machine learning to establish baselines of normal network behavior and alert on deviations.
    - Threat Hunting: Enables proactive search for threats within network data.
    - Threat Intelligence Integration: Enriches network data with threat intelligence for faster and more accurate detection.
- DNS Security:
    - Malicious Domain Blocking: Blocks access to known malicious domains (phishing, malware, C2 servers) at the DNS layer (e.g., Cisco Umbrella).
    - Domain Name System Security Extensions (DNSSEC): Protects against DNS spoofing and cache poisoning.
- DDoS Protection (Distributed Denial of Service):
    - Traffic Scrubbing: Diverts malicious traffic away from the target network, allowing only legitimate traffic to pass.
    - Rate Limiting: Controls the rate of incoming requests to prevent server overload.
- Secure Email Gateway:
    - Anti-Spam, Anti-Phishing, Anti-Malware: Protects against email-borne threats before they reach the inbox.
    - Data Loss Prevention (DLP): Prevents sensitive data from leaving the organization via email.
- Load Balancing and Application Delivery Controllers (ADCs):
    - Traffic Distribution: Distributes incoming network traffic across multiple servers to optimize performance and prevent overload.
    - SSL Offloading: Handles SSL/TLS encryption/decryption, reducing server load.
    - Web Application Firewall (WAF): Protects web applications from common web-based attacks (e.g., SQL injection, cross-site scripting).
- Security Information and Event Management (SIEM) / Security Orchestration, Automation, and Response (SOAR):
    - Centralized Log Management: Collects, aggregates, and correlates security logs and events from all network devices and systems.
    - Automated Response: Automates security workflows and incident response tasks.

4. User and Device Security

User and Device Security focuses on protecting individual users, their identities, and the endpoints they use to access organizational resources. It's critical in an environment with remote work, BYOD, and a distributed workforce.

- Multi-Factor Authentication (MFA) / Adaptive MFA:
    - Identity Verification: Requires users to provide multiple forms of verification (e.g., password + phone push, biometrics, security key) to confirm their identity.
    - Risk-Based Authentication: Adapts authentication strength based on contextual factors like location, device health, and access history.
- Zero Trust Network Access (ZTNA):
    - Identity-Based Access: Grants access to specific applications based on verified user identity and device posture, not network location.
    - Least-Privilege Access: Provides granular, just-in-time access to only the necessary resources.
    - Continuous Trust Verification: Continuously re-evaluates trust during a session.
- Endpoint Detection and Response (EDR) / Endpoint Protection Platform (EPP):
    - Advanced Malware Protection: Detects, blocks, and remediates advanced malware, ransomware, and fileless attacks on endpoints (laptops, desktops, servers, mobile devices).
    - Behavioral Analysis: Monitors endpoint activity for suspicious behaviors.
    - Threat Hunting: Enables proactive search for threats on endpoints.
    - Automated Response and Remediation: Isolates compromised devices and removes malicious artifacts.
- Data Loss Prevention (DLP) for Endpoints:
    - Sensitive Data Monitoring: Monitors user actions to prevent unauthorized copying, transferring, or printing of sensitive data from endpoints.
    - Policy Enforcement: Enforces policies to control how sensitive data is used and shared.
- Secure Web Gateway (SWG):
    - Web Content Filtering: Blocks access to malicious or inappropriate websites.
    - Cloud-delivered Security: Delivers web security as a cloud service to protect users regardless of location.
    - SSL/TLS Inspection: Inspects encrypted web traffic for hidden threats.

- Email Security:
    - Anti-Phishing and Anti-Spam: Protects users from email-borne threats that attempt to compromise credentials or deliver malware.
    - Impersonation Protection: Prevents social engineering attacks targeting users.
- Secure Browser / Remote Browser Isolation (RBI):
    - Web Session Isolation: Executes web Browse sessions in a remote, isolated container, protecting users from drive-by downloads and browser-borne exploits.
- Unified Endpoint Management (UEM) / Mobile Device Management (MDM):
    - Device Enrollment and Management: Manages and secures all types of endpoints (laptops, smartphones, tablets) across an organization.
    - Policy Enforcement: Enforces security policies (e.g., encryption, strong passwords, app control) on devices.
    - Remote Wipe/Lock: Provides capabilities to remotely wipe or lock lost or stolen devices.
- User Behavior Analytics (UBA) / User and Entity Behavior Analytics (UEBA):
    - Insider Threat Detection: Monitors user behavior to detect anomalies that may indicate insider threats, compromised accounts, or data exfiltration.
    - Risk Scoring: Assigns risk scores to user activities to prioritize suspicious behavior.
- Security Awareness Training:
    - Phishing Simulations: Trains users to identify and report phishing attempts.
    - Education: Educates users about common cyber threats and best security practices.

Collaboration Products

- Calling
- Contact Center
- Meetings
- Phones, headsets, and collaboration devices
- Services for collaboration
- View all collaboration products

Collaboration Products

1. Calling

Modern enterprise calling solutions go far beyond traditional desk phones, offering rich features that integrate voice communication into a broader collaboration ecosystem.

- Voice over IP (VoIP) & Cloud Calling:
    - Internet-based Communication: Leverages the internet to transmit voice calls, reducing costs associated with traditional phone lines (PSTN).
    - Cloud-based Infrastructure: Calls are routed and managed through cloud servers, providing scalability, reliability, and accessibility from anywhere with an internet connection.
    - Unified Dial Plan: A consistent dialing experience across the organization, regardless of user location or device.
- Advanced Call Management Features:
    - Call Routing: Intelligent routing of incoming calls based on predefined rules (e.g., time of day, caller ID, agent availability, skill level).
    - Call Forwarding & Simultaneous Ring: Directs calls to other numbers or devices, or rings multiple devices simultaneously.
    - Voicemail & Voicemail-to-Email/Text: Transcribes voicemails and sends them as text or audio files to email or messaging apps.
    - Caller ID: Displays detailed caller information, often integrated with corporate directories.
    - Do Not Disturb (DND): Temporarily blocks incoming calls.
    - Call Transfer (Blind & Consultative): Seamlessly transfers calls to another party, with the option to consult with the recipient first.
    - Call Hold & Music on Hold: Puts calls on hold and plays custom music or messages.
    - Call Park: Allows a user to park a call in a virtual location and pick it up from another device.
    - Call Groups/Delegation: Allows users to create groups that can receive calls on their behalf or delegate call answering to others.
- Unified Communications (UC) Integration:
    - Presence Status: Shows the availability of colleagues (e.g., online, in a meeting, busy, away).
    - Integrated Messaging: Seamlessly transitions from a call to a chat or vice versa.
    - Directory Integration: Easily search for and call contacts from within the platform.

    - Video Calling: Enables face-to-face video calls from the same calling application.
    - Screen Sharing: Allows users to share their screen during calls.
- Mobile & Desktop Clients (Softphones):
    - Flexible Access: Make and receive calls from laptops, desktops, tablets, or smartphones using a softphone application, eliminating the need for a physical desk phone.
    - Consistent Experience: Provides a uniform calling experience across all devices.
- Security & Compliance:
    - Encryption: Secures voice communication to prevent eavesdropping.
    - Emergency Calling (E911/112): Provides location support for first responders.
    - Call Recording: Records calls for quality assurance, training, and compliance.
- Analytics & Reporting:
    - Call Logs & Metrics: Provides data on call volume, duration, missed calls, and other key performance indicators (KPIs).

2. Contact Center

An enterprise contact center solution is a comprehensive platform designed to manage all customer interactions across multiple channels, streamline customer service operations, and enhance the customer experience.

- Omnichannel Communication:
    - Voice (Inbound/Outbound): Traditional phone calls.
    - Email: Handling customer inquiries and support via email.
    - Chat (Live Chat, Chatbots): Real-time text-based communication on websites or applications.
    - Social Media: Managing customer interactions and support via platforms like X (formerly Twitter), Facebook, etc.
    - SMS/Text Messaging: Support and notifications via text.
    - Self-Service Options: IVR, web portals, knowledge bases, FAQs that allow customers to find answers or resolve issues independently.
- Intelligent Routing:
    - Automatic Call Distribution (ACD): Distributes incoming interactions to available agents based on various criteria.

    - Skill-Based Routing: Directs customers to agents with the specific expertise needed to resolve their issue (e.g., language, product knowledge, problem type).
    - Caller ID Routing: Routes calls based on the caller's phone number or associated customer data.
    - Queue Management: Manages customer queues, provides wait time announcements, and offers options like virtual queuing or callbacks.
- Interactive Voice Response (IVR) Systems:
    - Automated Menus: Allows customers to interact with a system using voice commands or keypad inputs to navigate options, access information, or perform transactions without agent intervention.
    - Self-Service: Enables self-service for common queries (e.g., checking account balance, order status).
- Agent Productivity Tools:
    - Unified Agent Desktop: A single interface for agents to manage interactions across all channels, access customer information, and utilize internal knowledge bases.
    - CRM Integration: Seamlessly integrates with Customer Relationship Management (CRM) systems (e.g., Salesforce, HubSpot) to provide agents with a complete customer history ("screen pop" of customer data).
    - Knowledge Base Integration: Provides agents with quick access to relevant information to answer customer queries.
    - Automated Workflows: Automates repetitive tasks for agents.
    - Dialers (Predictive, Progressive, Preview): For outbound campaigns, automates dialing to maximize agent talk time.
- Workforce Management (WFM) & Optimization (WFO):
    - Forecasting & Scheduling: Predicts call volumes and schedules agents to meet demand, optimizing staffing levels.
    - Performance Monitoring: Tracks agent productivity, adherence, and performance against KPIs.
    - Quality Management (QM): Records and analyzes interactions for quality assurance, compliance, and agent coaching.
    - Gamification: Incentivizes agent performance through game-like elements.
- Analytics & Reporting:
    - Real-time Dashboards: Provides supervisors with live insights into contact center performance (e.g., call volume, wait times, agent status).
    - Historical Reporting: Analyzes past data for trends, agent performance, customer satisfaction (CSAT, NPS), and operational efficiency.

    - Speech and Text Analytics: Uses AI to analyze customer conversations (voice and text) for sentiment, keywords, and trends to identify pain points and opportunities.
- AI & Automation:
    - Chatbots & Virtual Assistants: Automate routine inquiries and provide self-service options.
    - AI-Powered Routing: Uses AI to further optimize call routing based on customer intent and agent fit.
    - Sentiment Analysis: Analyzes customer sentiment in real-time to help agents adjust their approach.
- Security & Compliance:
    - Data Encryption: Protects sensitive customer data.
    - PCI DSS, HIPAA, GDPR Compliance: Adheres to industry-specific regulations for data handling.
    - Call Recording & Archiving: Stores interactions for compliance and dispute resolution.

3. Meetings

Enterprise meeting platforms facilitate virtual and hybrid meetings, enabling real-time collaboration with high-quality audio, video, and a rich set of interactive tools.

- HD Audio and Video Quality:
    - High-Definition Streaming: Delivers clear, crisp audio and video for a professional meeting experience.
    - Noise Suppression & Echo Cancellation: Reduces background noise and prevents audio feedback for better clarity.
    - Adaptive Bandwidth Management: Adjusts quality based on network conditions to maintain connection stability.
- Screen Sharing & Presentation Tools:
    - Full Screen Sharing: Share entire desktop or specific applications.
    - Application Sharing: Share a specific application window.
    - Content Sharing: Share documents, presentations, and other files.
    - Remote Control: Allows a presenter to grant control of their screen to another participant.
- Interactive Collaboration Tools:
    - Whiteboarding: Virtual whiteboards for real-time brainstorming, drawing, and annotation.

    - Live Annotation: Allows participants to draw or highlight on shared content.
    - In-Meeting Chat: Text-based chat for questions, comments, and side conversations without interrupting the main discussion.
    - Polls & Q&A: Engage participants with interactive polls and a structured Q&A module.
    - Reactions/Emojis: Non-verbal feedback mechanisms.
- Meeting Management & Control:
    - Scheduling & Calendar Integration: Seamlessly schedule meetings directly from email clients (e.g., Outlook, Google Calendar).
    - Meeting Lobby/Waiting Room: Controls who enters a meeting and when.
    - Participant Management: Mute/unmute participants, remove participants, lock meetings.
    - Recording & Transcription: Records meeting audio, video, and shared content, often with AI-powered transcriptions and summaries.
    - Breakout Rooms: Divides large meetings into smaller groups for focused discussions.
- Security Features:
    - End-to-End Encryption (E2EE): Secures meeting content from interception.
    - Password Protection & SSO: Protects meetings with passwords and integrates with Single Sign-On (SSO) for secure access.
    - Role-Based Access Control: Assigns different permissions to hosts, co-hosts, and participants.
    - Data Privacy & Compliance: Adheres to privacy regulations (e.g., GDPR).
- AI Capabilities (Emerging):
    - Smart Summaries & Action Items: AI-generated meeting summaries and identified action items.
    - Real-time Translation: Provides live translation of spoken language.
    - Speaker Identification: Identifies who is speaking in the transcript.
- Scalability:
    - Support for Large Audiences: Accommodates hundreds or thousands of participants for webinars and large events.
- Integration with Other Tools:
    - Unified Communications Platform Integration: Seamlessly works with calling and messaging functionalities.
    - CRM/Project Management Integration: Integrates with other business applications for streamlined workflows.

4. Phones, Headsets, and Collaboration Devices

This category covers the hardware that enables seamless communication and collaboration, from personal devices to room-based systems.

- IP Phones (Desk Phones):
    - VoIP Connectivity: Connects directly to the internet to make calls.
    - HD Audio: Provides superior sound quality.
    - Programmable Buttons: Customizable buttons for speed dials, feature access, etc.
    - Speakerphone: Built-in speaker and microphone for hands-free calling.
    - Integration with Collaboration Platforms: Often designed to work seamlessly with specific UC platforms.
    - Video Capabilities (Video Phones): Some models include screens and cameras for video calling.
- Headsets (Wired & Wireless):
    - Noise-Canceling Microphones: Filters out background noise for clearer voice transmission.
    - High-Quality Audio: Delivers clear audio for calls and meetings.
    - Comfort & Ergonomics: Designed for extended wear.
    - Connectivity Options: USB, Bluetooth, 3.5mm jack.
    - Integrated Controls: Buttons for mute, volume, answer/end call directly on the headset.
- Dedicated Room-Based Video Conferencing Systems:
    - Integrated Cameras: High-resolution cameras with features like auto-framing and speaker tracking to keep participants in view.
    - Studio-Quality Microphones & Speakers: Optimized for room acoustics, with features like beamforming microphones to pick up voices clearly.
    - Large Displays: Connect to large screens for immersive video meetings.
    - Touch Controllers: Dedicated touch panels for easy meeting control (joining, sharing, muting).
    - Whiteboarding Capabilities: Often integrated with digital whiteboards for interactive sessions.
    - Wireless Content Sharing: Easily share content from laptops or mobile devices without cables.
    - Environmental Sensors: Some devices can monitor room occupancy, air quality, etc.
- Interactive Whiteboards/Displays:
    - Touch-Enabled Screens: Allow for direct annotation and drawing.
    - Built-in Collaboration Software: Often run collaboration applications

directly.
    - Integrated Cameras and Microphones: Function as all-in-one meeting devices.
- Webcams:
    - High-Definition Video: Provides clear video for personal or small group meetings.
    - Integrated Microphones: Basic audio capture.
    - Auto-Focus & Low-Light Correction: Enhances video quality in various conditions.
- All-in-One Video Bars:
    - Compact Design: Combines camera, microphone, and speakers into a single unit.
    - Simplified Deployment: Easy to set up in smaller meeting rooms or huddle spaces.
    - AI-Powered Features: Often include intelligent framing, noise suppression, and speaker tracking.
- Management & Security for Devices:
    - Centralized Device Management: Cloud-based portals to monitor, provision, update, and troubleshoot collaboration devices remotely.
    - Firmware Updates: Regular updates to ensure security and new features.
    - Device Integrity: Security features to protect the devices themselves from compromise.

5. Services for Collaboration

Collaboration services refer to the support, management, and strategic offerings that help organizations successfully implement, maintain, and optimize their collaboration solutions. These can be provided by vendors or specialized partners.

- Implementation and Deployment Services:
    - Planning & Design: Assessing organizational needs, designing the collaboration architecture (e.g., cloud, hybrid, on-premises), and network readiness assessments.
    - Configuration & Setup: Installing and configuring software, integrating with existing systems (e.g., identity management, CRM), and setting up network connectivity.
    - Data Migration: Migrating user data, contacts, and historical information.
- Managed Services:

    - Proactive Monitoring: 24/7 monitoring of collaboration infrastructure and services to identify and resolve issues before they impact users.
    - Remote Management: Remote configuration, troubleshooting, and optimization of collaboration systems.
    - Performance Optimization: Ensuring high quality of service (QoS) for voice and video, optimizing network performance.
    - Updates & Patch Management: Applying software updates and security patches to collaboration platforms and devices.
    - Reporting & Analytics: Providing regular reports on system performance, usage, and incident trends.
- Support Services:
    - Technical Support (Help Desk): Providing assistance to users and administrators for issues, troubleshooting, and how-to questions.
    - Tiered Support: Offering different levels of support based on severity and complexity.
    - SLA (Service Level Agreements): Guarantees on response times and resolution times.
- Training & Adoption Services:
    - User Training: Providing training programs for end-users on how to effectively use collaboration tools.
    - Administrator Training: Training IT staff on managing and troubleshooting the collaboration environment.
    - Change Management: Strategies to facilitate user adoption and ensure a smooth transition to new collaboration tools.
    - Best Practices & Workshops: Offering guidance on how to leverage collaboration features for improved productivity and teamwork.
- Integration Services:
    - Custom Integrations: Developing custom integrations between collaboration platforms and other line-of-business applications (e.g., CRM, ERP, HR systems).
    - API Development: Utilizing APIs to extend functionality and automate workflows.
- Security and Compliance Services:
    - Security Audits: Assessing the security posture of collaboration environments.
    - Compliance Consulting: Ensuring that collaboration solutions meet regulatory requirements (e.g., GDPR, HIPAA, PCI DSS).
    - Threat Mitigation: Providing services to address security vulnerabilities specific to collaboration.

- Consulting and Advisory Services:
    - Strategic Planning: Assisting organizations in developing a long-term collaboration strategy.
    - Technology Roadmapping: Helping plan future collaboration technology investments.
    - ROI Analysis: Demonstrating the return on investment for collaboration solutions.

6. View all collaboration products

This typically refers to a comprehensive portfolio or a unified platform that brings together all the above categories, offering a holistic solution for an organization's communication and collaboration needs. This might be a single vendor's entire collaboration suite (e.g., Cisco Webex Suite, Microsoft Teams ecosystem).

Key features of a "View all collaboration products" approach emphasize integration and completeness:

- Unified Platform:
    - Single User Experience: A consistent interface and user experience across calling, messaging, meetings, and device management.
    - Centralized Administration: A single administrative portal to manage all collaboration services and devices.
- Seamless Integration:
    - Interoperability: All components (calling, meetings, messaging, devices) work together seamlessly, allowing users to move fluidly between modes of communication.
    - Deep Integration with Business Applications: Connects with common business applications (CRM, productivity suites, project management tools).
- Scalability and Flexibility:
    - Cloud-based Delivery: Leverages the cloud for scalability, accessibility, and resilience, supporting a workforce that can be anywhere.
    - Hybrid Deployment Options: Supports organizations that require a mix of on-premises and cloud-based solutions.
- Advanced Analytics and Insights:
    - Cross-Collaboration Analytics: Provides holistic insights into usage patterns, performance metrics, and adoption rates across all

collaboration tools.
    - Workspace Intelligence: Insights into meeting room utilization, device health, and environmental factors.
- Security and Compliance:
    - End-to-End Security: Consistent security policies and encryption across all communication and data.
    - Integrated Identity Management: Strong authentication and access control across the entire suite.
    - Compliance Tools: Features to help meet various industry and regulatory compliance requirements.
- Rich Device Ecosystem:
    - Interoperable Hardware: Supports a wide range of certified phones, headsets, and room systems designed to work optimally with the platform.
    - Device Management: Centralized tools for managing and monitoring all collaboration hardware.
- AI-Powered Enhancements:
    - Intelligent Meetings: AI-driven features for noise reduction, transcription, summaries, and action items.
    - Virtual Assistants: AI assistance for scheduling, managing tasks, and answering questions.
- Customization and Extensibility:
    - APIs and SDKs: Allows organizations to customize the platform, build custom applications, or integrate with niche business tools.
    - Developer Ecosystem: Access to a developer community and resources for building custom solutions.

Featured Solution

- Webex Suite: Everything your business needs to collaborate—in the world's first unified, purpose-built suite for hybrid work.

Featured Solution

The Webex Suite is Cisco's comprehensive, unified collaboration solution, specifically designed and "purpose-built" to address the evolving needs of hybrid work environments. This means it's engineered to provide a seamless and inclusive experience for employees, whether they are working from home, in the office, or on

the go.

The core idea behind the Webex Suite is to consolidate multiple collaboration functionalities into a single, integrated platform, minimizing the need for businesses to juggle various disparate tools. This unification aims to boost productivity, simplify IT management, and enhance the overall user experience.

Key Features of the Webex Suite

1. Unified Collaboration Experience (The Webex App):
    - All-in-one Application: Users access calling, meetings, and messaging from a single, intuitive Webex App, reducing context switching and improving workflow.
    - Consistent Experience: Provides a uniform user interface and functionality across desktop, mobile, and Webex devices, ensuring a consistent experience regardless of where or how someone is working.
2. Robust Calling Capabilities:
    - Cloud Calling: Offers a complete business phone system delivered from the cloud, enabling users to make and receive calls from any device (desk phone, softphone on PC/mobile).
    - Advanced Call Features: Includes call routing, voicemail-to-email, call forwarding, hunt groups, and secure calling.
    - Webex Go: Allows users to make and receive business calls using their personal mobile phone's native dialer, without revealing their personal number.
3. Intelligent Meetings:
    - HD Audio and Video: Delivers high-quality audio and video for clear and engaging virtual meetings.
    - AI-Powered Features:
        - Noise Removal & Voice Optimization: Intelligently filters out background noise and enhances voice clarity.
        - AI Assistant & Smart Summaries: Automates note-taking, generates meeting highlights, action items, and personalized summaries, allowing participants to focus on the discussion.
        - Real-time Translation: Provides live translation of spoken conversations into over 100 languages, promoting inclusivity in global teams.
        - Gesture Recognition: Interprets hand gestures (e.g., thumbs up) for quick, non-verbal feedback.
        - People Focus & Immersive Share: Uses AI to intelligently frame speakers and integrate presenters directly into content,

enhancing engagement for remote participants.
    - Interactive Tools: Includes in-meeting chat, polls (via Slido), Q&A, and digital whiteboarding for dynamic collaboration.
    - Breakout Rooms: Facilitates smaller group discussions within larger meetings.
    - Scalability: Supports large numbers of participants for various meeting types.
4. Persistent Messaging:

    - Team Spaces: Creates dedicated spaces for ongoing team collaboration, file sharing, and project management.
    - Secure File Sharing: Allows users to securely share files within messaging spaces.
    - Digital Whiteboarding: Provides persistent digital whiteboards for brainstorming and design, accessible before, during, and after meetings.
    - Guest Access: Enables secure collaboration with external partners and clients.
5. Comprehensive Events and Webinars:

    - Webinars: Tools for hosting high-quality webinars for audiences of any size, with features for engagement and simplified management.
    - Webex Events (formerly Socio): A robust platform for managing virtual, in-person, and hybrid events, including multi-track agendas, ticketing, attendee networking, and analytics.
    - Live Polling & Q&A (Slido integration): Boosts audience engagement during webinars and events.
6. Optimized for Hybrid Workspaces and Devices:

    - Purpose-Built Devices: Seamless integration with a wide range of Cisco Webex devices, including IP Phones, headsets, Webex Desk Series, Webex Room Systems, and digital whiteboards. These devices often feature built-in AI for enhanced audio and video.
    - Touchless Meeting Experiences: Voice commands (Webex Assistant) and proximity sensing for easy, hands-free meeting control.
    - Workspace Management: Tools for managing meeting rooms, desk spaces, and hot desking, providing insights into utilization.
7. Enterprise-Grade Security and Management:

    - Security by Design: Built-in end-to-end encryption for meetings and messages, advanced privacy features, and compliance certifications.
    - Cisco Control Hub: A single, AI-powered management console for IT administrators to provision users, manage devices, troubleshoot issues, and gain real-time insights across the entire Webex Suite.

    - Compliance Tools: Helps organizations meet industry and regional regulatory requirements.
8. Extensibility and Integrations:

    - App Hub: Provides integrations with popular business applications (e.g., Microsoft 365, Google Workspace, Salesforce, Slack, Miro) to streamline workflows.
    - APIs and SDKs: Allows for custom integrations and development of unique applications.

Computing Products

- Converged infrastructure
- Fabric and adapters
- Hybrid cloud operations
- Hyperconverged infrastructure
- Servers
- Services for unified computing
- View all computing products

Computing Products

1. Converged Infrastructure (CI)

Converged Infrastructure is an IT framework that bundles together compute (servers), networking (switches), storage (storage arrays), and often virtualization software and management tools into a single, pre-configured, and pre-tested integrated solution. It's designed to simplify IT deployment, management, and scaling by overcoming the traditional silos of disparate hardware components.

- Pre-integrated and Pre-tested:

    - Single SKU Procurement: Components are acquired as a single product unit from a single vendor, simplifying purchasing.
    - Reduced Integration Effort: Hardware and software components are already validated to work together, eliminating compatibility issues and significantly reducing deployment time and complexity compared to assembling components from different vendors.
- Simplified Management:

    - Unified Management Interface: Often provides a single management console or software layer to oversee and control the integrated compute, storage, and networking resources. This streamlines day-to-day

operations and reduces the need for specialized expertise in each silo.
    - Automated Provisioning: Enables faster provisioning of resources and deployment of applications by automating many of the manual configuration tasks.
- Scalability:
    - Modular Expansion: Typically scales by adding additional pre-configured blocks or modules of compute, storage, and networking, simplifying expansion.
    - Predictable Performance: Designed to offer predictable performance due to the integrated and optimized nature of its components.
- Cost Efficiency (Operational):
    - Reduced Operational Costs: Simplifies management and troubleshooting, leading to lower IT operational expenditures (OpEx).
    - Faster Time to Value: Quicker deployment means applications and services can be brought online faster, benefiting the business.
- Vendor Reliance:
    - Single Vendor Support: Generally purchased from a single vendor, which can simplify support but also lead to vendor lock-in and potentially fewer customization options.
- Common Use Cases:
    - Often used for specific workloads like VDI (Virtual Desktop Infrastructure), enterprise applications (ERP, CRM), and private cloud deployments where a consistent, predictable environment is desired.

2. Fabric and Adapters

In the context of modern data centers and unified computing, "Fabric" refers to a high-speed, low-latency, and highly scalable network infrastructure that interconnects compute, storage, and networking resources. "Adapters" are the network interface cards (NICs) or host bus adapters (HBAs) that connect servers to this fabric.

- Unified Fabric (e.g., Cisco Unified Fabric):
    - Consolidated I/O: Unifies different types of network traffic (LAN, SAN, HPC) onto a single Ethernet-based fabric. This reduces the number of adapters, cables, and switches, simplifying the network architecture.
    - High Bandwidth and Low Latency: Designed for high-performance data transfer, critical for modern applications and virtualized environments.
    - Scalability: The fabric can scale out by adding more switches and

connections, providing ample bandwidth for growing data center needs.
    - Simplified Management: A unified fabric simplifies network management by consolidating different network types into a single, cohesive system, often managed from a central point.
    - Non-Blocking Architecture: Ensures that traffic can flow freely without bottlenecks, optimizing performance.
- Network Adapters (NICs) / Host Bus Adapters (HBAs) / Converged Network Adapters (CNAs):
    - High-Speed Connectivity: Provide the physical interface for servers to connect to the network fabric (e.g., 10 Gigabit Ethernet, 25GE, 40GE, 100GE, InfiniBand).
    - Converged Network Adapters (CNAs): A specialized type of adapter that combines the functionality of a NIC (for LAN traffic) and an HBA (for Fibre Channel storage traffic) onto a single card. This further reduces the number of adapters and cables needed in a server, simplifying cabling and freeing up PCIe slots.
    - Offload Engines: Many adapters include hardware offload capabilities to reduce CPU utilization for network and storage processing (e.g., iSCSI offload, TCP/IP offload).
    - Virtualization Support: Optimized for virtualized environments, supporting features like SR-IOV (Single Root I/O Virtualization) to improve performance and efficiency for virtual machines.
    - Quality of Service (QoS): Enables prioritization of different types of traffic (e.g., FCoE for storage, VoIP for voice) to ensure critical applications receive the necessary bandwidth.

3. Hybrid Cloud Operations

Hybrid cloud operations involve managing and orchestrating workloads, data, and applications across a mix of on-premises infrastructure, private cloud environments, and one or more public cloud services. The goal is to provide seamless integration, consistent management, and optimal placement of workloads based on business needs (e.g., cost, performance, compliance, security).

- Unified Management Plane:
    - Single Pane of Glass: A consolidated management platform that allows IT teams to monitor, deploy, and manage resources across different cloud environments (on-premises, private, public) from a single interface.
    - Orchestration and Automation: Automates the deployment, scaling, and management of applications and infrastructure across the hybrid environment, reducing manual effort and errors.

- Workload Mobility:
    - Seamless Migration: Enables easy and secure migration of applications and data between on-premises and cloud environments, as well as between different public clouds.
    - Containerization (e.g., Kubernetes): Utilizes container orchestration platforms (like Kubernetes) to create portable applications that can run consistently across any cloud environment.
- Consistent Networking and Security:
    - Software-Defined Networking (SDN): Extends network policies and segmentation consistently across hybrid environments.
    - Unified Security Policies: Applies consistent security policies, compliance controls, and identity management across all cloud environments to maintain a strong security posture.
    - Data Encryption: Ensures data is encrypted in transit and at rest across all locations.
- Data Management and Storage:
    - Data Tiering and Archiving: Strategically places data in the most cost-effective and performant storage tiers across hybrid environments.
    - Data Synchronization and Replication: Ensures data consistency and availability across multiple locations for disaster recovery and business continuity.
- Cost Optimization and Visibility:
    - Cost Analytics: Provides tools to monitor and optimize cloud spending across different providers.
    - Resource Utilization Tracking: Offers visibility into resource consumption to ensure efficient allocation and prevent over-provisioning.
- Developer and DevOps Enablement:
    - Consistent Development Environment: Provides developers with a consistent environment for building and deploying applications, regardless of the underlying infrastructure.
    - CI/CD Pipeline Integration: Integrates with Continuous Integration/Continuous Delivery (CI/CD) pipelines to automate the deployment of applications to hybrid environments.

4. Hyperconverged Infrastructure (HCI)

Hyperconverged Infrastructure is a software-defined IT infrastructure that virtualizes all the elements of conventional "hardware-defined" systems (compute, storage, and often networking) into a single, integrated software stack running on industry-standard x86 servers. It fundamentally differs from CI by tightly integrating these components at the hypervisor level.

- Software-Defined Everything:
    - Compute (Hypervisor): Leverages a hypervisor (e.g., VMware vSphere, Microsoft Hyper-V, Nutanix AHV) to virtualize compute resources.
    - Software-Defined Storage (SDS): Storage functions are managed by software running on each node, pooling local storage resources across the cluster to form a distributed storage fabric. This eliminates the need for separate, dedicated storage arrays.
    - Software-Defined Networking (SDN - often integrated or integrated-ready): Network virtualization and policy enforcement are increasingly integrated into the HCI stack.
- Simplified Management:
    - Single Management Plane: HCI systems are managed through a single, intuitive interface (often integrated with the hypervisor management console), which controls all compute, storage, and networking resources. This drastically simplifies operations.
    - VM-centric Management: Resources are often provisioned and managed at the virtual machine (VM) level, simplifying operations for virtualized workloads.
- Scalability:
    - Modular ("Scale-Out") Growth: HCI scales by simply adding more "nodes" (servers) to the cluster. This allows for incremental, on-demand growth of both compute and storage resources.
    - Linear Scalability: Performance and capacity generally scale linearly as nodes are added, providing predictable expansion.
- Data Efficiency and Protection:
    - Inline Deduplication & Compression: Optimizes storage usage by removing redundant data and compressing it in real-time.
    - Built-in Data Protection: Often includes integrated backup, replication, and disaster recovery capabilities (e.g., snapshots, remote replication), reducing the need for separate backup solutions.
    - Data Locality: Keeps data close to the compute resources that use it, minimizing latency and improving performance.
- Cost Efficiency (Both CapEx and OpEx):

    - Reduced Hardware Footprint: Eliminates the need for separate storage arrays and dedicated SAN switches, reducing capital expenditures (CapEx).
    - Lower Power and Cooling: Fewer hardware components lead to reduced power and cooling costs.
    - Simplified Operations: Significantly lowers operational expenditures (OpEx) due to simplified management and automation.
- Flexibility and Agility:

    - Rapid Deployment: HCI clusters can be deployed and operational much faster than traditional infrastructure.
    - Supports Various Workloads: Ideal for virtualized environments, VDI, remote office/branch office (ROBO), edge computing, and private cloud deployments.

5. Servers

Servers are powerful computers designed to provide services, resources, and data to other computers (clients) over a network. Enterprise servers are built for high performance, reliability, scalability, and security to meet the demanding requirements of business-critical applications and data.

- High Performance and Processing Power:

    - Multiple CPUs/Cores: Equipped with multiple high-performance processors and numerous cores to handle demanding workloads and parallel processing.
    - Large Memory Capacity (RAM): Supports vast amounts of RAM to efficiently run multiple applications and virtual machines concurrently.
    - High-Speed Internal Buses: Optimized internal architecture for rapid data transfer between components.
- Reliability and High Availability (HA):

    - Redundant Components: Features redundant power supplies, cooling fans, and often network adapters to ensure continuous operation even if a component fails.
    - Hot-Swappable Components: Allows for the replacement of components (e.g., power supplies, hard drives, fans) while the server is running, minimizing downtime.
    - Error-Correcting Code (ECC) Memory: Automatically detects and corrects memory errors, enhancing data integrity and system stability.
    - RAID (Redundant Array of Independent Disks): Protects data by

distributing it across multiple disks, allowing the system to continue operating even if one drive fails.
    - Clustering Support: Designed to work in clusters for failover and load balancing, ensuring continuous service availability.
- Scalability:
    - Vertical Scaling (Scale-Up): Ability to add more CPUs, RAM, and storage within the same server chassis.
    - Horizontal Scaling (Scale-Out): Designed to work effectively in large groups or clusters, allowing for the addition of more servers to distribute workloads and increase capacity.
- Advanced Management Features:
    - Lights-Out Management (e.g., IPMI, iLO, iDRAC): Remote management capabilities that allow administrators to monitor, configure, power on/off, and troubleshoot the server even when the operating system is down.
    - Centralized Management Tools: Integration with management platforms for monitoring large fleets of servers.
    - Predictive Analytics: Increasingly includes features that use AI/ML to predict hardware failures before they occur.
- Security:
    - Hardware-Root-of-Trust: Built-in security features at the hardware level to ensure the integrity of the server's firmware and boot process.
    - Secure Boot: Ensures that only trusted software can load during the boot process.
    - Encryption Capabilities: Hardware-level support for data encryption.
    - TPM (Trusted Platform Module): Hardware-based security for cryptographic keys and secure boot.
- Form Factors:
    - Rack Servers: Designed to be mounted in standard server racks, optimizing space and cooling in data centers.
    - Blade Servers: Modular servers that fit into a shared chassis, sharing power, cooling, and networking infrastructure for high density and simplified cabling.
    - Tower Servers: Standalone servers suitable for smaller businesses or specific remote office deployments.

6. Services for Unified Computing

"Services for Unified Computing" generally refer to the support, consulting, and managed services that complement and optimize Unified Computing System (UCS) environments (like Cisco UCS) or similar integrated computing platforms. These services help organizations design, deploy, manage, and maintain their converged or hyperconverged infrastructure effectively.

- Planning and Design Services:
    - Assessment: Evaluating existing IT infrastructure, business needs, and workload requirements.
    - Architecture Design: Designing the optimal UCS or unified computing architecture, including sizing, topology, and integration with existing systems (storage, networking, virtualization).
    - Migration Planning: Developing strategies for migrating applications and data to the new unified computing environment.
- Implementation and Deployment Services:
    - Installation and Configuration: Physical installation of hardware (servers, fabric interconnects) and configuration of software components (firmware, network policies, storage profiles).
    - Integration: Connecting UCS with existing data center infrastructure, virtualization platforms (e.g., VMware vCenter), and management tools.
    - Proof of Concept (PoC): Deploying a small-scale environment to validate functionality and performance.
- Managed Services:
    - Remote Monitoring: 24/7 monitoring of UCS health, performance, and alerts.
    - Patching and Firmware Updates: Proactive management and application of firmware and software updates to ensure security and stability.
    - Configuration Management: Ensuring consistent configuration across the unified computing environment.
    - Performance Optimization: Tuning the UCS environment for optimal performance of applications and workloads.
    - Troubleshooting and Support: Providing expert support for issue resolution and problem diagnosis.
- Optimization and Advisory Services:
    - Health Checks and Audits: Periodic assessments of the UCS environment to identify potential issues, best practice deviations, and areas for improvement.
    - Capacity Planning: Analyzing usage trends and forecasting future capacity needs to ensure the environment can scale with business

growth.
    - Workload Placement Optimization: Advising on the best placement of applications and workloads within the unified computing environment (or across hybrid cloud).
    - Automation Strategy: Helping organizations leverage UCS's automation capabilities for operational efficiency.
- Training and Enablement:
    - Technical Training: Providing training for IT staff on operating, managing, and troubleshooting the unified computing system.
    - Knowledge Transfer: Ensuring the in-house IT team has the necessary skills to manage the environment independently.
- Security and Compliance Services:
    - Security Configuration Review: Auditing UCS configurations against security best practices and compliance requirements.
    - Vulnerability Management: Identifying and addressing vulnerabilities within the unified computing stack.
- Lifecycle Management:
    - Hardware Refresh Planning: Assisting with planning and executing hardware upgrades and replacements.
    - End-of-Life/End-of-Support Guidance: Providing strategies for managing hardware and software lifecycle transitions.

7. View all computing products

This category represents the vendor's complete portfolio of computing solutions, emphasizing how they integrate and work together to provide a comprehensive and flexible infrastructure. For a vendor like Cisco, this often means highlighting the synergy between their UCS servers, Nexus networking, storage integrations, and management software.

Key aspects of a "View all computing products" approach:

- Holistic Portfolio: Presents a complete ecosystem of servers, fabric interconnects, network adapters, and management software designed to work together.
- Integrated Architecture: Emphasizes how individual products (e.g., UCS servers, Nexus switches) combine to form a cohesive, unified computing architecture.
- Flexibility in Deployment: Highlights support for various deployment models:
    - On-Premises: Traditional data center deployments.
    - Hybrid Cloud: Integration with public cloud providers.

    - Edge Computing: Solutions for smaller, distributed environments.
- Centralized Management: Showcases a common management platform (e.g., Cisco Intersight) that spans across different computing products and environments (on-premises, cloud, edge).
- Automation and Orchestration: Underscores the ability to automate provisioning, configuration, and lifecycle management across the entire computing stack.
- Performance and Scalability: Emphasizes the high performance, low latency, and ability to scale resources to meet demanding enterprise workloads.
- Security: Highlights integrated security features across the entire computing stack, from hardware roots of trust in servers to secure networking and management.
- Ecosystem Integrations: Details compatibility and integration with various virtualization platforms (VMware, Hyper-V, Kubernetes), operating systems, and enterprise applications.
- Lifecycle Management: Comprehensive support from planning and deployment through ongoing operations, optimization, and eventual refresh.

Featured Solution

- Cisco Intersight: Get simplified IT operations with infrastructure lifecycle management as a service

Cisco Intersight is a cloud-based (SaaS - Software-as-a-Service) hybrid cloud operations platform designed to simplify and automate the lifecycle management of IT infrastructure. It provides a unified management experience for Cisco's compute (UCS, HyperFlex) and networking platforms, along with integration for third-party servers, storage, virtualization, and container platforms.

The core promise of Intersight is to provide "simplified IT operations with infrastructure lifecycle management as a service." This means moving away from traditional, fragmented management tools to a more intelligent, proactive, and automated approach delivered from the cloud.

Key Features and Benefits of Cisco Intersight

1. Unified Global Management (Single Pane of Glass):

    - Consolidated View: Provides a centralized dashboard to monitor and manage Cisco UCS (Unified Computing System) servers, Cisco HyperFlex hyperconverged infrastructure, Cisco networking platforms, and increasingly, third-party infrastructure and public cloud services.
    - Global Visibility: Offers at-a-glance insights into the health, status,

inventory, and performance of infrastructure assets across various locations (data centers, remote sites, branch offices, edge environments).
    - Customizable Dashboards: Allows IT teams to create personalized dashboards with relevant metrics and widgets to suit their specific operational needs.
2. Infrastructure Lifecycle Management as a Service:
    - SaaS Delivery: As a cloud-delivered platform, Intersight eliminates the need for customers to deploy and maintain on-premises management software. Updates, new features, and patches are automatically delivered by Cisco, ensuring IT teams always have the latest capabilities.
    - Deployment Options: While primarily SaaS, Intersight also offers a Connected Virtual Appliance (CVA) for those who prefer an on-premises footprint with cloud connectivity, and a Private Virtual Appliance (PVA) for air-gapped or highly secure environments requiring full data locality.
3. Intelligent Automation and Orchestration:
    - Model-Based Configuration: Simplifies provisioning and deployment by allowing IT staff to create reusable server profiles and policies. These profiles define consistent configurations (e.g., BIOS settings, firmware versions, network settings, storage profiles) that can be applied to single servers or hundreds of servers, regardless of form factor.
    - Workflow Designer: Features a drag-and-drop workflow designer to automate complex, multi-step IT operations across compute, storage, networking, and virtualization. It includes a library of pre-built tasks and supports integration with third-party automation tools (e.g., Ansible, Terraform) via open APIs.
    - Operating System (OS) Installation Automation: Automates the unattended installation of operating systems on Cisco UCS servers.
4. Proactive Monitoring and Observability:
    - Real-time and Historical Metrics: Collects extensive telemetry data to provide detailed insights into infrastructure performance, resource utilization, and health.
    - Health and Fault Monitoring: Continuously monitors the health of all managed systems, detects faults, and generates alerts, helping IT teams stay ahead of problems.
    - Predictive Analytics: Uses embedded analytics to identify potential hardware failures or performance issues before they impact users or applications.
    - Hardware Compatibility List (HCL) Compliance: Automatically checks hardware and firmware configurations against Cisco's HCL to ensure compliance and supportability, alerting users to unsupported

configurations.

5. Enhanced Support Experience:
    - Proactive Support: Automatically opens service requests and generates technical support files to the Cisco Technical Assistance Center (TAC) for detected faults, significantly accelerating troubleshooting and resolution.
    - Smart Call Home Integration: Further automates the support process, reducing the burden on IT staff.
    - Advisories: Provides security and technical advisories relevant to the managed infrastructure.
6. Security and Compliance:
    - Role-Based Access Control (RBAC): Granular control over user permissions to ensure only authorized personnel can perform specific actions.
    - Multi-Factor Authentication (MFA) & SSO: Supports strong identity verification for secure access to the Intersight platform.
    - Audit Logging: Logs all actions taken on the infrastructure for security auditing and compliance.
    - Firmware Management: Centralized management of firmware versions and automated upgrades helps maintain a secure and compliant posture.
    - Power Management: Allows setting and applying power policies at the server or chassis level to optimize power consumption and manage cooling.
7. Extensibility and Integration:
    - Open API (RESTful API): Provides a robust and programmable API that supports the OpenAPI Specification (OAS), enabling deep integration with other IT operations management (ITOM) tools, DevOps pipelines, and custom applications.
    - SDKs: Offers Python and PowerShell SDKs for easier integration with automation frameworks like Ansible, Chef, and Puppet.
    - Ecosystem Integrations: Connects with third-party solutions for storage, virtualization (e.g., VMware vCenter), and other services.

In essence, Cisco Intersight aims to transform IT operations from a reactive, manual, and siloed approach to a proactive, automated, and unified strategy, ultimately allowing IT teams to focus more on innovation and less on mundane infrastructure management tasks.

Observability Products

- Application performance management
- Application security
- Internet, cloud, and endpoint visibility
- Workload optimization
- Services for observability

Observability Products

1. Application Performance Management (APM)

APM focuses specifically on monitoring and managing the performance and availability of software applications. It aims to detect, diagnose, and resolve performance issues and bottlenecks before they impact end-users or business operations.

- Real-time Performance Monitoring:
    - Response Time & Throughput: Tracks how quickly applications respond to user requests and the volume of requests they can handle.
    - Error Rates: Monitors the frequency of application errors.
    - Resource Utilization: Tracks CPU, memory, disk I/O, and network usage by the application and its underlying infrastructure.
    - User Experience Monitoring (Real User Monitoring - RUM): Collects data from actual user interactions to understand performance from the end-user's perspective (e.g., page load times, click-through rates, geographical performance).
    - Synthetic Monitoring: Simulates user interactions with applications from various locations to proactively identify performance issues before real users encounter them.
- Distributed Tracing:
    - End-to-End Transaction Visibility: Tracks the complete path of a request as it flows through multiple microservices, databases, and network components in a distributed architecture.
    - Latency Identification: Pinpoints where latency is occurring within the transaction flow, helping to identify bottlenecks.
    - Root Cause Analysis: Provides a detailed trace of events, enabling rapid identification of the root cause of performance degradations or failures.
- Code-Level Diagnostics and Profiling:
    - Deep Code Insights: Pinpoints performance issues down to specific lines of code, database queries, or external API calls.
    - Method-Level Visibility: Profiles application code to identify inefficient

algorithms or resource-intensive functions.

- Application Dependency Mapping:
    - Automated Discovery: Automatically discovers and maps the relationships and dependencies between various application components, services, databases, and infrastructure.
    - Topology Visualization: Provides visual maps of the application architecture, which is crucial for understanding complex microservices environments.
- Alerting and Anomaly Detection:
    - Customizable Alerts: Allows setting thresholds for key performance indicators (KPIs) and receiving notifications when these thresholds are breached.
    - Baseline and Anomaly Detection: Learns normal application behavior and automatically flags deviations that could indicate a problem, even for unknown issues.
    - Intelligent Alerting: Reduces alert fatigue by correlating related alerts and prioritizing critical issues.
- Database Monitoring:
    - Query Performance: Monitors database query execution times, slow queries, and database resource utilization.
    - Connection Pooling: Tracks database connection usage and efficiency.
- Infrastructure Monitoring Integration:
    - Full-Stack Visibility: Integrates with underlying infrastructure monitoring (servers, VMs, containers, cloud resources) to provide a holistic view of application performance in context.
- Business Transaction Monitoring:
    - Business Impact: Links application performance directly to business outcomes (e.g., conversion rates, revenue).
    - Service Level Agreements (SLAs) / Service Level Objectives (SLOs): Monitors performance against predefined service level targets.

2. Application Security (AppSec)

Application Security products focus on identifying, preventing, and mitigating security vulnerabilities within applications throughout their entire lifecycle, from design and development to deployment and runtime.

- Static Application Security Testing (SAST):

    - Source Code Analysis: Analyzes application source code, bytecode, or binary code *without executing it* to identify potential security vulnerabilities (e.g., SQL injection, cross-site scripting, buffer overflows) during the development phase.
    - Early Detection: Helps developers find and fix vulnerabilities early in the Software Development Life Cycle (SDLC), reducing the cost of remediation.
- Dynamic Application Security Testing (DAST):
    - Runtime Analysis: Tests running applications by simulating attacks from the outside, similar to how a malicious hacker would. It identifies vulnerabilities accessible via the application's interface (e.g., web pages, APIs).
    - Black-Box Testing: Does not require access to source code and can test third-party applications.
- Interactive Application Security Testing (IAST):
    - Hybrid Analysis: Combines elements of SAST and DAST. It operates within the running application (e.g., using an agent) to analyze code execution and data flow from within, providing more precise vulnerability identification and context than DAST, and covering more ground than SAST alone.
- Software Composition Analysis (SCA):
    - Open Source Security: Identifies open-source components, libraries, and dependencies used in an application and checks them against known vulnerability databases (e.g., CVEs).
    - License Compliance: Helps manage open-source license compliance risks.
- Runtime Application Self-Protection (RASP):
    - In-App Protection: Embeds security capabilities directly into the application runtime environment. RASP actively monitors application behavior and can detect and block attacks in real-time by analyzing requests and application logic from within.
    - Protection Against Zero-Day Attacks: Can protect against unknown vulnerabilities and attacks by understanding application behavior.
- API Security Testing:
    - API Vulnerability Scanning: Specifically designed to test the security of APIs, which are common attack vectors in modern microservices architectures.

    - Authentication and Authorization Testing: Verifies the robustness of API access controls.
- Web Application Firewall (WAF):
    - Perimeter Protection: Sits in front of web applications, filtering and monitoring HTTP traffic between a web application and the Internet. It protects web applications from common web-based attacks (e.g., SQL injection, XSS, DDoS).
- Container Security / Cloud-Native Application Security:
    - Image Scanning: Scans container images for vulnerabilities and misconfigurations.
    - Runtime Protection: Monitors container and Kubernetes environments for suspicious activity and enforces security policies.
- Threat Modeling:
    - Proactive Threat Identification: A structured approach to identify potential threats and vulnerabilities early in the design phase of an application.
- Centralized Reporting and Remediation Guidance:
    - Vulnerability Prioritization: Helps prioritize remediation efforts based on severity and business impact.
    - Integration with DevOps/CI/CD: Seamlessly integrates security testing into the development pipeline for automated checks.

3. Internet, Cloud, and Endpoint Visibility

This category focuses on providing comprehensive visibility into network traffic, cloud environments, and individual user devices (endpoints) to detect threats, monitor performance, and ensure compliance across distributed IT landscapes.

- Network Visibility (Internet/Cloud/On-Premises):
    - Traffic Monitoring: Captures and analyzes network flow data (NetFlow, sFlow, IPFIX) and packet data for deep insights into communication patterns.
    - Performance Monitoring: Identifies network latency, packet loss, and bandwidth bottlenecks.
    - Threat Detection: Detects anomalous traffic patterns, command-and-control (C2) communication, data exfiltration, and other indicators of compromise (IoCs).
    - DNS Monitoring: Tracks DNS queries to detect malicious domains and C2

activity.
    - Encrypted Traffic Analysis (ETA/Decryption): Identifies malware in encrypted traffic without decryption (using behavioral analytics) or decrypts traffic for deeper inspection where necessary.
    - Application-Aware Networking: Identifies and prioritizes application traffic.
- Cloud Visibility (Public Cloud Environments):
    - Cloud Infrastructure Monitoring: Monitors the health, performance, and configuration of cloud resources (VMs, containers, serverless functions, databases, storage) in IaaS, PaaS, and SaaS environments.
    - Cloud Security Posture Management (CSPM): Continuously monitors cloud configurations against security best practices and compliance benchmarks to identify misconfigurations and risks.
    - Cloud Native Logging and Metrics: Collects and analyzes logs and metrics from cloud services and applications.
    - Cloud Traffic Flow Visibility: Provides insights into traffic between virtual networks, services, and public endpoints within and across cloud providers.
    - Cost Optimization Visibility: Tracks and analyzes cloud spending across services and accounts.
- Endpoint Visibility:
    - Endpoint Detection and Response (EDR): Continuously monitors endpoint activity (processes, file changes, network connections, user behavior) for malicious activity.
    - Threat Hunting: Enables security analysts to proactively search for threats across endpoint data.
    - Incident Response: Provides tools for isolating compromised endpoints, collecting forensic data, and initiating remediation actions.
    - Device Inventory and Health: Maintains an up-to-date inventory of all connected endpoints and their security posture (e.g., patch level, antivirus status).
    - User Behavior Analytics (UBA/UEBA): Monitors user activity on endpoints to detect anomalous behavior that might indicate insider threats or compromised accounts.
- Unified Dashboard and Correlation:
    - Centralized Data Aggregation: Gathers telemetry data (metrics, logs, traces) from all these diverse sources into a single platform.
    - Cross-Domain Correlation: Correlates events and data across network, cloud, and endpoint domains to provide a holistic view of potential threats or performance issues, enabling faster root cause analysis.

- Automated Remediation (Orchestration):
    - Automated Responses: Can trigger automated actions (e.g., quarantining an endpoint, blocking an IP address, adjusting cloud firewall rules) based on detected anomalies or threats.

4. Workload Optimization

Workload optimization focuses on intelligently allocating and managing resources to ensure that applications and services (workloads) run efficiently, perform optimally, and meet their service level objectives while minimizing operational costs. It's about getting the "right resources at the right time at the right cost."

- Resource Allocation and Balancing:
    - Dynamic Resource Assignment: Automatically adjusts CPU, memory, storage, and network resources allocated to workloads in real-time based on demand.
    - Workload Balancing: Distributes workloads across available infrastructure to prevent resource contention, avoid bottlenecks, and ensure optimal performance.
    - Intelligent Placement: Recommends or automatically moves workloads to the most suitable infrastructure (e.g., specific hosts, clusters, or even different cloud regions) based on performance, cost, and compliance policies.
- Capacity Planning and Forecasting:
    - Demand Forecasting: Analyzes historical usage patterns and growth trends to predict future resource needs.
    - "What-if" Scenario Analysis: Allows administrators to model the impact of new workloads or changes to infrastructure before implementation.
    - Resource Sizing: Helps right-size virtual machines and containers to prevent over-provisioning (wasted resources) or under-provisioning (performance issues).
- Performance Assurance:
    - Automated Actions: Takes automated actions (e.g., vMotion, adding resources, scaling out) to maintain workload performance and ensure SLAs are met.
    - Constraint Management: Ensures that optimization decisions respect defined policies, compliance requirements, and business priorities.
    - Real-time Optimization: Continuously monitors and optimizes resource allocation in real-time based on changing workload demands.

- Cost Optimization (FinOps):
    - Cloud Cost Management: Identifies opportunities to reduce cloud spend by rightsizing instances, identifying idle resources, and optimizing storage tiers.
    - On-Premises Efficiency: Maximizes the utilization of on-premises hardware, delaying the need for new capital expenditures.
    - Licensing Optimization: Helps ensure compliance and efficient use of software licenses.
- Policy-Driven Automation:
    - Business Intent: Allows defining policies based on business goals (e.g., "prioritize performance for critical applications," "optimize cost for development environments").
    - Automated Governance: Enforces these policies automatically across the infrastructure.
- Integration with Virtualization and Cloud Platforms:
    - Hypervisor Integration: Deep integration with virtualization platforms (e.g., VMware vSphere, Microsoft Hyper-V, Kubernetes) to directly control virtual resources.
    - Public Cloud Integration: Connects with major public cloud providers (AWS, Azure, GCP) to manage and optimize workloads across hybrid and multi-cloud environments.
- Reporting and Analytics:
    - Optimization Recommendations: Provides clear, actionable recommendations for resource adjustments.
    - Impact Analysis: Shows the potential impact of proposed optimizations on performance and cost.

5. Services for Observability

"Services for Observability" encompass the professional, managed, and consulting services that help organizations implement, manage, and mature their observability practices. These services are provided by vendors or specialized partners to ensure an organization can effectively collect, analyze, and act upon telemetry data.

- Observability Strategy and Assessment:
    - Current State Analysis: Assessing an organization's existing monitoring capabilities, tooling, and operational processes.
    - Maturity Assessment: Evaluating the organization's current observability

maturity level.
    - Roadmap Development: Designing a comprehensive observability strategy aligned with business objectives, including tool selection, data collection architecture, and team training.
- Implementation and Onboarding:
    - Platform Deployment: Assisting with the deployment and configuration of observability platforms (SaaS or on-premises).
    - Instrumentation: Helping developers and SREs instrument applications (e.g., adding SDKs, agents) to emit metrics, logs, and traces.
    - Data Ingestion and Integration: Configuring data pipelines to collect telemetry data from diverse sources (applications, infrastructure, cloud services, network devices, security tools) and ingest it into the observability platform.
    - Dashboard and Alert Configuration: Setting up meaningful dashboards, visualizations, and intelligent alerts tailored to specific business needs and technical requirements.
- Managed Observability Services:
    - 24/7 Monitoring and Alerting: Proactive monitoring of the observability platform itself and the underlying systems it observes.
    - Alert Triage and Incident Escalation: Managing alerts, filtering noise, and escalating critical incidents to appropriate teams.
    - Platform Maintenance: Managing updates, upgrades, and patching of the observability platform components.
    - Performance Tuning: Optimizing the observability platform for scale and performance.
    - Data Management: Managing data retention, storage, and cost optimization for telemetry data.
- Observability Engineering and Customization:
    - Custom Instrumentation Development: Creating custom instrumentation for unique applications or legacy systems.
    - Custom Dashboard and Report Creation: Developing specialized dashboards and reports for specific stakeholders or use cases.
    - Workflow Automation: Integrating observability insights into existing IT operations and DevOps workflows.
    - API Integration: Developing custom integrations with other ITOM, security, or business intelligence tools via APIs.
- Training and Enablement:
    - Developer Training: Training developers on how to instrument their code for observability.

    - SRE/Operations Training: Training operations and SRE teams on how to use the observability platform for troubleshooting, performance analysis, and incident response.
    - Observability Best Practices: Guiding teams on adopting best practices for metrics, logging, tracing, and alert management.
- Advanced Analytics and AIOps Integration:
    - Anomaly Detection Configuration: Tuning anomaly detection algorithms for specific environments and workloads.
    - Root Cause Analysis Assistance: Providing expertise in using observability data for deeper root cause analysis.
    - AIOps Integration: Helping integrate observability data with AIOps platforms for predictive insights, automated incident correlation, and proactive problem resolution.
- Compliance and Governance:
    - Data Retention Policies: Helping define and enforce data retention policies for observability data to meet compliance requirements.
    - Security Best Practices: Ensuring the observability platform itself and its data collection mechanisms adhere to security best practices.

Featured Solution

- Splunk AppDynamics: Get complete application awareness across the technology stack and monitor application performance across multicloud environments

Featured Solution

Splunk AppDynamics is a leading Application Performance Management (APM) and observability solution that offers deep, end-to-end visibility into the performance, health, and security of applications, particularly in complex, distributed, and multi-cloud environments. Its core strength lies in providing "complete application awareness across the technology stack."

This means it doesn't just tell you *if* an application is slow, but *why* it's slow, *where* the bottleneck is, and *how* that issue impacts your business. With its integration into the broader Splunk Observability Cloud portfolio, it offers a more unified view across logs, metrics, and traces.

Key Capabilities of Splunk AppDynamics for Complete Application Awareness and Multicloud Monitoring:

1. Automatic Discovery and Mapping of Business Transactions and Application Topologies:
    - End-to-End Transaction Tracing: AppDynamics automatically discovers and maps the entire flow of user requests (known as "business transactions") as they traverse through various application components, services (including microservices), databases, caches, and third-party APIs.
    - Dynamic Flow Maps: It creates real-time, visual dependency maps that show how all application components interact, highlighting connections and dependencies, even in highly dynamic and distributed architectures. This helps operations teams quickly understand the application's architecture and identify problematic areas.
    - Code-Level Visibility: For instrumented applications, AppDynamics can drill down to the code level, pinpointing specific methods, classes, and database queries that are causing performance bottlenecks.
2. AI-Powered Performance Baselines and Anomaly Detection:
    - Dynamic Baselines: Instead of static thresholds, AppDynamics uses machine learning to automatically learn the normal performance behavior of each application, service, and business transaction. This creates "dynamic baselines" that adapt to changes in usage patterns.
    - Proactive Anomaly Detection: It automatically identifies deviations from these dynamic baselines (anomalies) in real-time, alerting IT teams to performance issues *before* they significantly impact end-users or service levels. This significantly reduces alert noise.
    - Root Cause Analysis: When an anomaly is detected, AppDynamics intelligently correlates the issue to the underlying cause, often down to a specific service, infrastructure component, or line of code, accelerating mean time to resolution (MTTR).
3. Digital Experience Monitoring (DEM):
    - Real User Monitoring (RUM): Collects data directly from end-users' browsers and mobile devices to provide insights into their actual experience, including page load times, JavaScript errors, network latency, and geographical performance. This allows businesses to understand the impact of performance issues on customer journeys.
    - Synthetic Monitoring: Proactively simulates user interactions from various global locations to test application availability and performance 24/7, even when real users aren't active. This helps identify issues before they affect customers.
    - Session Replay: For some issues, AppDynamics can capture video recordings of user sessions, allowing teams to visually replay and

understand the sequence of actions that led to a problem.

4. Full-Stack Observability and Integration:
    - Infrastructure Monitoring: Integrates with underlying infrastructure monitoring (servers, VMs, containers, cloud resources) to correlate application performance with the health and utilization of the compute, storage, and network layers.
    - Database Visibility: Provides deep insights into database performance, including slow queries, connection issues, and resource contention.
    - Log Context (with Splunk integration): Through "Log Observer Connect for AppDynamics," it provides deep links from application performance data in AppDynamics directly to relevant logs in Splunk Enterprise or Splunk Cloud Platform. This allows teams to seamlessly pivot from a performance issue to its underlying log events for faster root cause analysis ("what, when, where" from AppD, "why" from Splunk logs).
    - Network Intelligence (with Cisco ThousandEyes): Integrates with Cisco ThousandEyes to provide visibility into external network paths, internet outages, and SaaS application performance, completing the end-to-end view of the digital supply chain.
5. Multicloud and Hybrid Cloud Monitoring:
    - Broad Coverage: Designed to monitor applications and infrastructure deployed across various environments, including on-premises data centers, private clouds, and multiple public cloud providers (AWS, Azure, GCP, etc.).
    - Cloud-Native Support: Supports monitoring of modern cloud-native architectures, including microservices, containers (Docker, Kubernetes), and serverless functions.
    - Consistent Visibility: Provides a consistent monitoring experience regardless of where the application components reside, allowing teams to manage hybrid and multi-cloud environments effectively without relying on disparate tools.
6. Business iQ (Business Performance Monitoring):
    - Business Context: Links application performance metrics directly to key business outcomes (e.g., conversion rates, revenue, customer satisfaction, order completion). This allows IT teams to understand the real-world business impact of performance issues and prioritize remediation efforts based on financial or customer experience implications.
7. Application Security (Secure Application):
    - Runtime Application Self-Protection (RASP): Provides real-time

vulnerability detection and protection against attacks directly within the application runtime environment.
    - Business Risk Prioritization: Correlates security vulnerabilities and attacks with their potential business impact, helping security and development teams prioritize remediation efforts.
8. Scalability and Flexibility:

    - Distributed Architecture: Built to scale and handle the massive data volumes generated by large, complex enterprise applications and distributed systems.
    - OpenTelemetry Support: Embraces open standards for telemetry data collection, providing flexibility and avoiding vendor lock-in for data ingestion.

Software Products

- Networking Software
    - Catalyst Center
    - Catalyst SD-WAN Manager
    - IoT Operations Dashboard
    - Meraki Platform
    - Nexus Dashboard
    - All networking software

Networking Software

1. Cisco Catalyst Center (formerly Cisco DNA Center)

Cisco Catalyst Center is an advanced, AI-powered network management and automation platform that simplifies the management of Cisco Catalyst network infrastructure (wired and wireless LAN, SD-WAN). It provides a centralized, intent-based approach to connect, secure, and automate network operations, ensuring a consistent user experience.

- Intent-Based Networking (IBN):

    - Abstraction and Policy Enforcement: Allows administrators to define network behavior in high-level business terms (intent) rather than configuring individual devices. Catalyst Center then translates this intent into device-specific configurations and ensures policy enforcement across the network.
    - Network Assurance: Continuously monitors network health and performance, comparing the actual network state against the defined intent. It proactively identifies deviations, predicts issues, and provides

actionable insights for troubleshooting.

- Network Automation and Provisioning:
    - Zero-Touch Provisioning (ZTP): Automates the onboarding and configuration of new network devices (switches, access points, routers) without manual intervention, significantly speeding up deployment.
    - Workflow Automation: Automates routine operational tasks such as software image upgrades, security policy deployment, and network changes, reducing human error and operational costs.
    - Policy-Driven Automation: Allows for the creation and automated deployment of network policies (e.g., QoS, segmentation, access control) across the entire network.
- Visibility and Analytics (AIOps):
    - End-to-End Visibility: Provides a granular, unified view of the entire network, including devices, clients, applications, and their interactions, from a single dashboard.
    - AI/ML-Driven Insights: Leverages Artificial Intelligence and Machine Learning to analyze network telemetry data (NetFlow, syslog, SNMP, streaming telemetry) to detect anomalies, predict performance degradation, and offer prescriptive recommendations for faster problem resolution.
    - Application Experience Monitoring: Provides deep insights into application performance and the end-user experience, helping to identify and resolve application-related network issues.
    - Client Health Monitoring: Monitors individual client devices (wired and wireless) to assess their connectivity, performance, and compliance posture.
- Integrated Security:
    - Network Segmentation: Facilitates micro-segmentation and macro-segmentation policies to isolate users, devices, and applications, limiting the lateral movement of threats.
    - Zero Trust Network Access (ZTNA): Supports the implementation of Zero Trust principles by enforcing identity-based policies and continuously verifying trust.
    - Encrypted Traffic Analytics (ETA): Detects malware and threats in encrypted network traffic without decrypting it, using advanced analytics and behavioral analysis.
    - Integration with Cisco Security Products: Seamlessly integrates with security solutions like Cisco Identity Services Engine (ISE) for identity-based access control and Cisco Stealthwatch for network visibility and threat detection.

- Open and Extensible:
    - APIs: Provides a rich set of open REST APIs to integrate with third-party systems, IT Service Management (ITSM) tools, DevOps pipelines, and other orchestration platforms, enabling broader IT automation.
    - Ecosystem Integration: Supports integration with a wide range of Cisco and third-party solutions for a unified management experience.
- Sustainability Features: Enables smart building initiatives and optimizes Power over Ethernet (PoE) infrastructure for energy efficiency.

2. Cisco Catalyst SD-WAN Manager (formerly Cisco vManage)

Cisco Catalyst SD-WAN Manager is the centralized management plane for Cisco's Catalyst SD-WAN solution (formerly Viptela SD-WAN). It provides a highly customizable and automated dashboard for deploying, configuring, managing, monitoring, and operating the entire SD-WAN fabric.

- Centralized Orchestration and Control:
    - Single Pane of Glass: Offers a unified web-based interface to manage the entire SD-WAN overlay network, including routers (WAN Edges), controllers (vSmart, vBond), and policies.
    - Zero-Touch Provisioning (ZTP): Automates the onboarding and deployment of SD-WAN devices at branch offices and remote sites, simplifying large-scale rollouts.
- Policy-Driven Configuration:
    - Granular Policy Creation: Allows administrators to define and apply granular, intent-based policies for routing, QoS (Quality of Service), security, and traffic engineering across the entire SD-WAN fabric.
    - Application-Aware Routing: Intelligently routes application traffic over the best available WAN link based on real-time network conditions (latency, jitter, packet loss) and application requirements, ensuring optimal performance for critical applications.
    - Topology Control: Allows administrators to design and enforce network topologies (e.g., full mesh, hub-and-spoke) for different business needs.
- Deep Visibility and Monitoring:
    - Real-time Analytics: Provides real-time visibility into WAN link performance, application performance, and network health.
    - Network-Wide Path Insights (NWPI): Visualizes traffic flows and data paths across the WAN, aiding in troubleshooting and performance analysis.

    - SD-WAN Analytics: Ingests network data and uses machine learning to predict capacity trends and identify potential issues.
    - Troubleshooting Tools: Offers a rich set of built-in tools for diagnosing and resolving WAN performance issues.
- Integrated Security:
    - Centralized Security Policy Management: Allows for consistent application of security policies (e.g., firewall rules, intrusion prevention) across all SD-WAN branches.
    - Encrypted VPN Tunnels: Establishes secure, encrypted tunnels between SD-WAN devices over any transport (MPLS, internet, LTE).
    - Direct Internet Access (DIA) with Security: Enables secure direct internet access from branches with integrated security services to optimize cloud application performance while maintaining security.
- Software Management:
    - Centralized Software Upgrades: Simplifies the process of upgrading software images on all SD-WAN devices across the fabric.
- Programmability and Automation:
    - REST APIs: Provides comprehensive REST APIs, allowing for programmatic interaction, automation of tasks, and integration with third-party orchestration and management systems.
- Scalability and High Availability:
    - Clustered Deployment: Supports clustered deployments for high availability and redundancy of the management plane.
    - Multi-Tenancy: Can be deployed in a multi-tenant mode to support service provider environments.

3. Cisco IoT Operations Dashboard

Cisco IoT Operations Dashboard is a cloud-based service designed to simplify the secure deployment, monitoring, and management of industrial networking devices and connected industrial assets (sensors, machines) at massive scale. It's built for operational technology (OT) teams and IT support staff to gain insights from their IoT deployments.

- Centralized Cloud-Based Management:
    - Unified Dashboard: Provides a single, cloud-based dashboard for managing a large fleet of Cisco industrial routers (e.g., IR1101, IR1800 series) and other IoT devices.

    - Simplified Deployment: Enables fast and secure deployment of IoT networks, often leveraging Zero-Touch Provisioning (ZTP) for industrial routers.
    - Scalability: Designed to manage thousands to millions of distributed IoT devices and assets.
- Industrial Networking Device Management:
    - Remote Monitoring: Provides real-time visibility into the status, health, and location of industrial networking devices on a map.
    - Configuration Management: Allows for remote configuration and management of industrial router settings, including network policies, VPNs, firewall rules, and interface configurations.
    - Firmware Management: Facilitates remote scheduling and execution of firmware upgrades for industrial devices over the air or via wired connections.
    - Troubleshooting: Offers IoT-specific alerts and tools for proactive and reactive remote troubleshooting of field IoT devices.
- Secure Equipment Access:
    - Granular Remote Access: Enables secure, controlled remote access to operational equipment behind managed gateways, crucial for remote maintenance and troubleshooting by in-house teams or third-party technicians.
    - Access Control: Provides granular access controls based on user roles and specific devices, limiting access to authorized personnel and defined methods (SSH, HTTPS).
    - Secure Tunneling: All provisioning and management traffic occurs over encrypted IPSec tunnels.
- Industrial Asset Visibility and Insights:
    - Asset Management: Allows for discovery, inventory, and mapping of industrial assets and sensors.
    - Sensor Monitoring: Monitors data from connected industrial sensors, providing insights into operational conditions (e.g., temperature, pressure, vibration).
    - LoRaWAN Integration: Supports integration with LoRaWAN wireless gateways for industrial asset vision.
    - Data Orchestration (Edge to Multi-Cloud): Enables secure data flow from edge devices to various cloud platforms for further analysis and integration with business applications.
- Security and Compliance:
    - Encrypted Communication: Ensures all user and device traffic to the

dashboard is encrypted.
    - Certificate-Based Authentication: Secures device registration and claiming processes.
    - Single Sign-On (SSO) and Multi-Factor Authentication (MFA): Enhances user login security.
    - Role-Based Access Control (RBAC): Assigns different permission levels to users (administrator, operator, monitor).
    - Audit Trail: Maintains detailed logs of user-initiated actions and device events for compliance and security forensics.
- Alerting and Notifications:

    - Customizable Alerts: Allows setting up IoT-specific alerts for various conditions.
    - Role-Based Notifications: Sends email or SMS notifications to specific groups or individuals based on alert categories or device groups.

4. Cisco Meraki Platform

The Cisco Meraki Platform is renowned for its 100% cloud-managed networking and IT solutions, offering a unified, simplified management experience across a wide range of hardware products, including wireless access points, switches, security appliances (SD-WAN), security cameras, and mobile device management.

- 100% Cloud-Managed Architecture:

    - Meraki Dashboard: A centralized, web-based dashboard provides a single interface for monitoring, configuring, and troubleshooting the entire Meraki network globally.
    - No On-Premises Controllers: Eliminates the need for separate hardware controllers for wireless, switching, or security, simplifying deployment and reducing operational overhead.
    - Automatic Firmware Updates: Firmware updates are delivered and managed automatically from the cloud, ensuring devices are always up-to-date with the latest features and security patches.
- Zero-Touch Provisioning (ZTP):

    - Plug-and-Play Deployment: Devices can be shipped directly to a site, plugged in, and automatically configured from the cloud dashboard, significantly accelerating deployment times.
- Unified Management Across Product Families:

    - Wireless (MR Access Points): Cloud-managed Wi-Fi with AI-driven optimization (Auto RF, Adaptive Radio Management) for seamless

performance, guest Wi-Fi, and location analytics.
    - Switching (MS Switches): Cloud-managed access and aggregation switches with features like virtual stacking, port security, and PoE control, all managed from the dashboard.
    - Security & SD-WAN (MX Security Appliances): Unified Threat Management (UTM) capabilities (firewall, IPS, content filtering, AMP), built-in site-to-site VPN, and intelligent SD-WAN for optimized connectivity and reduced MPLS costs.
    - Smart Cameras (MV Security Cameras): Cloud-managed video surveillance with onboard analytics (motion detection, people counting, heat maps), no NVRs required, and secure cloud archiving.
    - Mobile Device Management (Systems Manager): Centrally manages and secures mobile devices (iOS, Android, macOS, Windows), enforces security policies, distributes apps, and provides remote wipe/lock capabilities.
    - Sensors (MT Sensors): Smart IoT sensors for environmental monitoring (temperature, humidity, leaks, open/close) integrated into the same dashboard.
- Deep Visibility and Analytics:
    - Real-time Insights: Provides real-time data on network health, device performance, client usage, and security threats.
    - Application Visibility: Layer 7 application visibility and control allows for granular traffic shaping and policy enforcement based on application type.
    - Actionable Analytics: Offers detailed performance metrics and custom reports, often with AI-driven insights, to help with proactive troubleshooting and data-driven IT decisions.
- Advanced Security Features:
    - Integrated Threat Intelligence: Leverages Cisco Talos threat intelligence for real-time protection against emerging cyber threats.
    - Advanced Malware Protection (AMP): Built-in malware detection and prevention.
    - Identity-Based Policies: Granular control over network access based on user roles, device types, and application usage.
    - Automated VPNs: Simplifies the creation of secure VPN tunnels between sites.

5. Cisco Nexus Dashboard

Cisco Nexus Dashboard is a unified platform designed to simplify the management,

automation, and assurance of data center networks, particularly for Cisco's Application Centric Infrastructure (ACI), Nexus Dashboard Fabric Controller (NDFC), and standalone NX-OS switches. It acts as a central operational console for hybrid cloud data center environments.

- Unified Operational Console:
    - Single Pane of Glass: Provides a consolidated view and management point for multiple data center fabrics and sites, whether they are ACI, NDFC (LAN/SAN/IPFM), or standalone NX-OS deployments.
    - Consistent Experience: Offers a consistent user experience and shared services across different data center domains.
- Microservices-Based Architecture:
    - Scalability and Resilience: Built on a microservices architecture, allowing for independent scaling of services and enhanced resilience.
    - Seamless Upgrades: Enables non-disruptive upgrades of the platform and its services.
    - Deployment Flexibility: Available in various form factors including physical appliances (Cisco UCS hardware), virtual machines (VMware ESXi, KVM), and public cloud deployments (AWS, Azure).
- Integrated Observability and Assurance Services:
    - Nexus Dashboard Insights (NDI): Provides real-time network telemetry, AI/ML-driven analytics, and proactive troubleshooting. It offers deep insights into network health, performance, and behavior, helping to identify and resolve issues quickly.
    - Network Assurance Engine (NAE): (Often part of the Insights offering) Verifies network correctness and compliance against design intent, performing continuous verification and providing "what-if" analysis for changes.
- Multi-Fabric Automation and Orchestration:
    - Nexus Dashboard Orchestrator (NDO): Enables centralized policy orchestration and automation across multiple ACI and NDFC fabrics, simplifying consistent policy deployment across geographically dispersed data centers or hybrid cloud environments.
    - Nexus Dashboard Fabric Controller (NDFC): (Inherited from DCNM) Provides centralized control and automation for NX-OS-based LAN (VXLAN, vPC), SAN, and IP Fabric for Media (IPFM) environments.
- Enhanced Day-2 Operations:
    - Operational Simplicity: Streamlines common operational tasks, reducing

complexity and human error.
    - Troubleshooting Tools: Offers advanced troubleshooting capabilities by correlating data across fabrics and services.
    - Compliance Checks: Continuously checks network configurations against defined compliance policies.
- Security and Integration:
    - Single Sign-On (SSO) and RBAC: Provides consistent user management, authentication, and role-based access control across all services on the dashboard.
    - Open APIs: Offers robust RESTful APIs for integration with third-party automation tools, ITSM platforms, and cloud orchestration systems.
    - Common Authentication Domains: Simplifies user management across different applications.

6. All Networking Software

This category represents the comprehensive breadth of a vendor's software solutions for networking. It highlights the synergy and complementary nature of the individual products, often presented as a unified portfolio.

Key characteristics when a vendor highlights "All Networking Software" are:

- Comprehensive Portfolio: Encompasses solutions for various network domains (Campus/Branch, WAN, Data Center, IoT, Cloud) and management paradigms (cloud-managed, on-premises controllers, cloud-native).
- Unified Management Strategy: While individual products have their specific consoles, the vendor aims to provide a cohesive management strategy across them, often through integration points, shared APIs, or overarching platforms (like Cisco Digital Network Architecture (DNA) or Nexus Dashboard).
- Automation Across Domains: Emphasis on automating workflows and operations across different network segments, from device provisioning to policy enforcement and troubleshooting.
- End-to-End Visibility: The collective power of these tools provides complete visibility from the end-user device to the application, across the campus, WAN, internet, and data center.
- Integrated Security: Security features are woven throughout the entire software stack, from segmentation and threat detection in Catalyst Center to encrypted tunnels in SD-WAN and API security in cloud network management.
- Hybrid and Multi-Cloud Readiness: Solutions are designed to support and manage networks that span on-premises infrastructure, private clouds, and various public cloud environments.
- Openness and Extensibility: Commitment to open APIs, developer communities,

and integration with a broad ecosystem of third-party tools and applications.
- AI/ML Driven Insights: Increasing adoption of AI and Machine Learning across the portfolio to provide predictive analytics, automate root cause analysis, and enhance operational intelligence.

- Security Software
  - Cyber Vision
  - Secure Equipment Access
  - Security Cloud

Security Software

1. Cisco Cyber Vision

Cisco Cyber Vision is an Industrial Control System (ICS) and Operational Technology (OT) security solution specifically designed to provide continuous visibility and threat detection for industrial networks. It helps organizations in sectors like manufacturing, energy, and transportation secure their critical infrastructure and ensure operational resilience and safety.

- Continuous OT Visibility and Asset Discovery:
  - Deep Packet Inspection (DPI) for Industrial Protocols: Uniquely monitors industrial network traffic by passively capturing and deeply decoding a wide range of OT protocols (e.g., Modbus, OPC, DNP3, Ethernet/IP, Siemens S7). This provides granular insights into communications.
  - Automated Asset Inventory: Automatically discovers and inventories all connected industrial assets, including their types, vendors, models, serial numbers, firmware versions, vulnerabilities, communication patterns, and network locations. This builds a real-time, comprehensive asset list.
  - Topology Mapping: Dynamically generates and visualizes the OT network topology, showing how devices are connected and communicating. This helps in understanding the control network's structure and identifying unauthorized connections.
- OT Security Posture and Risk Management:
  - Vulnerability Detection: Identifies known hardware and software vulnerabilities within OT devices and systems by comparing discovered assets against vulnerability databases (e.g., CVEs, NVD).
  - Risk Scoring: Automatically calculates risk scores for individual devices, components, and specific segments of the industrial operation, helping organizations prioritize remediation efforts based on potential impact.

Each score comes with guidance on how to reduce exposure.
    - Intrusion and Anomaly Detection: Leverages behavioral analytics and threat intelligence (from Cisco Talos) to detect abnormal communication patterns, unauthorized device access, unexpected variable changes, controller modifications, and known threats.
    - Compliance Reporting: Provides reports that assist organizations in meeting industry standards and regulatory compliance requirements for OT security.
- Integrated IT/OT Security Operations:
    - Seamless Integration with IT Security Tools: Shares rich OT context (asset details, vulnerabilities, communication flows) with IT security operations centers (SOCs) and platforms like Security Information and Event Management (SIEMs), firewalls (e.g., Cisco Secure Firewall), and Identity Services Engine (ISE). This enables a unified view of IT and OT security.
    - Automated Network Segmentation: Facilitates the creation of network segmentation policies by grouping assets into logical zones and automatically sharing this information with enforcement points like Cisco Secure Firewall or Cisco ISE for granular access control and threat containment.
- Operational Insights for OT Teams:
    - Process Event Monitoring: Decodes industrial protocols to track process events, asset modifications, and variable changes, providing OT engineers with real-time insights into the actual status of industrial processes.
    - Troubleshooting Assistance: Helps OT teams quickly troubleshoot production issues and maintain uptime by identifying network problems, device misconfigurations, and communication failures.
    - OT Flight Recorder: Maintains a historical record of all events, application flows, and variable accesses, enabling forensic investigations and incident reporting.
- Flexible Deployment Model:
    - Edge Monitoring Architecture: Leverages Cisco industrial network equipment (e.g., Catalyst Industrial Routers and Switches with Cyber Vision sensors) for distributed monitoring at the edge of the industrial network, eliminating the need for dedicated security appliances or complex SPAN collection networks.
    - Centralized Global Center: Aggregates data from multiple local sensors and sites to provide CISOs and security teams with centralized visibility across the entire industrial landscape.

2. Cisco Secure Equipment Access (SEA)

Cisco Secure Equipment Access is a cloud-managed, Zero Trust Network Access (ZTNA) solution specifically designed to provide secure, simplified, and granular remote access to Operational Technology (OT) assets and other industrial equipment. It allows authorized personnel (employees, contractors, vendors) to remotely access machinery and systems without exposing the entire OT network to the internet.

- Zero Trust Network Access (ZTNA) for OT:
    - Default Deny Posture: Starts with a "default deny" posture, meaning no access is granted until explicitly permitted.
    - Identity and Context-Based Access: Access is granted based on verified user identity, device posture, and contextual factors (e.g., time of day, purpose of access), rather than just network location.
    - Least Privilege Access: Ensures users are granted access only to the specific devices, protocols, and timeframes they need, minimizing the attack surface.
    - Micro-segmentation: Hides OT assets from network discovery, making lateral movement within the industrial network extremely difficult for unauthorized users.
- Simplified Remote Access Workflow:
    - Cloud Portal Management: A centralized cloud portal (often integrated with Cisco IoT Operations Dashboard) manages gateways and configures remote access policies for all industrial assets.
    - Easy Onboarding: Simplifies the onboarding of industrial switches and routers (acting as ZTNA gateways) into the system.
    - Multiple Access Methods: Supports various remote access methods including SSH, RDP, VNC, Telnet, and Web applications.
    - Agent-Based ZTNA (SEA Plus): For advanced tasks, SEA Plus establishes a secure IP communication channel between the user's computer and the OT asset, enabling the use of native desktop applications (e.g., PLC programming software, file transfer clients) without a full VPN.
- Enhanced Security and Compliance:
    - Secure Tunneling: All remote access traffic is secured via encrypted tunnels (e.g., DTLS, IPSec), protecting data in transit.
    - No IP Exposure in iDMZ: Industrial DMZs (iDMZs) are critical for securing OT networks; SEA avoids exposing OT IP addresses directly to the iDMZ, further reducing the attack surface.
    - Session Recording: Provides the ability to record remote access sessions (video recordings stored in customer-provided cloud storage like AWS S3), enhancing accountability, facilitating forensics, and aiding in

compliance.
    - Audit Trails: Maintains detailed logs of all remote access sessions, user actions, and policy enforcements for auditing and compliance purposes.
    - Role-Based Access Control (RBAC): Granular user roles (e.g., System Admin, Access Admin, User) define permissions and capabilities within the SEA platform.
- Scalability for Industrial Environments:
    - Built for OT Scale: Designed to deploy secure remote access to a large number of distributed OT assets across multiple industrial sites.
    - Integration with Industrial Networking: Embeds ZTNA gateway functionality directly into Cisco industrial switches and routers, simplifying deployment and reducing hardware footprint.
- Operational Benefits:
    - Reduced Downtime: Enables faster troubleshooting and maintenance by allowing remote access to equipment, reducing the need for on-site visits.
    - Improved Efficiency: Streamlines access for internal teams and external contractors, boosting operational efficiency.
    - Enhanced IT/OT Collaboration: Provides a secure and controlled mechanism for IT teams to assist OT personnel with industrial asset management.

3. Cisco Security Cloud

Cisco Security Cloud represents Cisco's evolving vision for a unified, cloud-delivered security platform designed to protect organizations from the network edge to any cloud, and across all users, applications, and devices. It aims to integrate and converge Cisco's vast security portfolio into a seamless, intelligent, and open architecture.

- Converged Security Platform (SSE & Beyond):
    - Security Service Edge (SSE) Capabilities: Offers a comprehensive suite of cloud-delivered security services, typically including:
        - Zero Trust Network Access (ZTNA): Securely connects users to private applications without placing them on the network, enforcing least privilege.
        - Secure Web Gateway (SWG): Filters and inspects web traffic, protecting users from malicious websites and enforcing web usage policies.
        - Cloud Access Security Broker (CASB): Discovers and controls sanctioned and unsanctioned SaaS applications, enforces data loss

prevention (DLP), and protects against threats in cloud environments.
        - Firewall as a Service (FWaaS): Provides cloud-delivered firewall capabilities for consistent policy enforcement across distributed networks and clouds.
    - Beyond SSE: Extends beyond basic SSE to incorporate broader security capabilities like:
        - Data Loss Prevention (DLP): Identifies and prevents the unauthorized transmission of sensitive data across various channels.
        - DNS Security (e.g., Cisco Umbrella): Blocks malicious domains at the DNS layer before connections are established.
        - Remote Browser Isolation (RBI): Isolates risky web content in a remote browser environment, preventing malware from reaching the user's device.
        - Malware Analysis: Advanced capabilities for detecting and analyzing sophisticated malware.
- Unified Policy Management and Orchestration:
    - Centralized Control Plane: Provides a single, cloud-native console for defining, enforcing, and managing security policies consistently across all security services and environments (on-premises, multi-cloud, remote users).
    - Policy Automation: Automates the deployment and enforcement of security policies, reducing manual effort and human error.
- Hybrid and Multi-Cloud Protection:
    - Consistent Security Across Environments: Extends security policies and controls seamlessly from on-premises networks to various public cloud providers (AWS, Azure, GCP) and SaaS applications.
    - Cloud Workload Protection (CWPP): Protects cloud-native workloads, containers, and serverless functions throughout their lifecycle.
    - Cloud Security Posture Management (CSPM): Continuously monitors cloud configurations for misconfigurations and compliance deviations.
- Threat Intelligence and Advanced Threat Protection:
    - Cisco Talos Integration: Leverages global threat intelligence from Cisco Talos (one of the world's largest commercial threat intelligence teams) for real-time protection against known and emerging threats.
    - Advanced Malware Protection (AMP): Detects, analyzes, and blocks sophisticated malware across endpoints, networks, and email.
    - Behavioral Analytics: Uses AI/ML to detect anomalous user and entity behavior (UEBA) and identify insider threats or compromised accounts.

    - XDR (Extended Detection and Response): Integrates telemetry from endpoints, networks, cloud, email, and identity to provide holistic threat detection, investigation, and response capabilities.
- Identity-Centric Security:
    - Multi-Factor Authentication (MFA) & Adaptive Authentication (e.g., Cisco Duo): Enforces strong identity verification with adaptive policies based on user context and risk.
    - Continuous Trust Verification: Continuously verifies user and device trust throughout a session.
    - Secure Access: Ensures that only authenticated and authorized users and devices can access corporate resources.
- Simplified Operations and Observability:
    - Centralized Visibility: Offers a real-time, unified view of threats and security posture across the entire digital ecosystem.
    - Automated Incident Response: Enables faster detection, investigation, and automated remediation of security incidents.
    - User Experience Insights: Integrates with tools like Cisco ThousandEyes to provide insights into user experience and application performance, helping to identify and resolve security-related performance issues.
- Open and Extensible Ecosystem:
    - APIs and Integrations: Provides open APIs for integration with third-party security tools (e.g., SIEMs, SOAR platforms), ITSM systems, and DevOps pipelines.
    - Modular Architecture: Allows organizations to consume security services modularly as needed, providing flexibility and scalability.

Observability Software

- Splunk AppDynamics
- Thousand Eyes

Observability Software: Detailed Key Features

1. Splunk AppDynamics

Splunk AppDynamics is a comprehensive Application Performance Management (APM) and observability solution that provides end-to-end visibility into the performance, health, and security of applications, especially in complex, distributed, and multi-cloud

environments. Its strength lies in providing "complete application awareness across the technology stack."

- Application Performance Monitoring (APM):
    - End-to-End Transaction Tracing: Automatically discovers and maps all business transactions as they flow through various application components, microservices, databases, and third-party APIs. This provides a detailed, hop-by-hop view of every request.
    - Code-Level Visibility: Drills down into the application code to pinpoint the exact line of code, database query, or external call causing performance bottlenecks or errors.
    - Dynamic Baselines and Anomaly Detection: Uses machine learning to automatically learn the normal performance behavior of applications and individual transactions. It then proactively flags deviations from these baselines, reducing alert noise and identifying issues before they impact users.
    - Automatic Root Cause Analysis: Correlates performance issues with underlying infrastructure, code, or network problems to help identify the root cause quickly and efficiently.
- Digital Experience Monitoring (DEM):
    - Real User Monitoring (RUM): Collects data from actual user interactions (browser, mobile devices) to understand front-end performance, page load times, JavaScript errors, and user journeys from their perspective.
    - Synthetic Monitoring: Proactively simulates user interactions from various global locations to test application availability and performance 24/7, providing early warnings of potential issues.
    - User Journey Maps: Visualizes how users navigate through applications, highlighting popular paths and areas where performance degradation might be impacting their experience.
- Business Performance Monitoring (Business iQ):
    - Business Transaction Correlation: Links application performance directly to key business metrics and outcomes, such as conversion rates, revenue, or customer satisfaction. This helps IT teams prioritize issues based on their business impact.
    - Impact Analysis: Quantifies the financial or operational impact of performance degradations, enabling data-driven decision-making.
- Full-Stack Observability & Ecosystem Integration:
    - Infrastructure Monitoring: Provides visibility into the underlying infrastructure (servers, VMs, containers, cloud services) that support the

applications, correlating infrastructure health with application performance.
    - Database Monitoring: Monitors database performance, including query execution times, resource utilization, and connection issues.
    - Log Context Integration (with Splunk Platform): Seamlessly links application performance data in AppDynamics to relevant logs in Splunk Enterprise or Splunk Cloud Platform, enabling quicker root cause analysis by providing rich contextual log data.
    - Network Performance Integration (with Cisco ThousandEyes): Offers combined insights into application and network performance, including external network paths, internet outages, and SaaS application dependencies (more on this below).
    - Container and Kubernetes Monitoring: Provides deep visibility into containerized applications, their performance, and resource consumption within Kubernetes environments.
- Application Security (Secure Application):
    - Runtime Application Self-Protection (RASP): Embeds security capabilities directly into the application runtime to detect and block attacks in real-time, providing protection against known and zero-day vulnerabilities.
    - Vulnerability Detection: Identifies security vulnerabilities in applications during runtime and provides context for remediation.
- Multi-Cloud and Hybrid Cloud Monitoring:
    - Supports monitoring of applications and infrastructure deployed across on-premises data centers, private clouds, and multiple public cloud environments (AWS, Azure, GCP), providing consistent visibility regardless of deployment location.

2. ThousandEyes

ThousandEyes is a network intelligence platform that provides unparalleled visibility into the performance of internet, cloud, and SaaS applications. It allows organizations to understand the factors outside their direct control (like ISP outages, BGP routing issues, or cloud provider network performance) that impact user experience and application availability.

- End-to-End Network Path Visibility (Internet and WAN):
    - Hop-by-Hop Path Visualization: Visualizes the complete network path from the user's device or an agent to any application or service, including paths across the public internet, cloud provider networks, and enterprise

WANs. This includes detailed information about each hop, such as latency, packet loss, and jitter.
    - BGP Monitoring: Monitors global BGP (Border Gateway Protocol) routing tables to detect route hijacks, leaks, and other routing anomalies that can impact reachability and performance to critical applications and services.
    - DNS Monitoring: Tracks DNS resolution performance and availability, identifying issues that can prevent users from accessing applications.
    - QoS Visibility: Provides insights into Quality of Service (QoS) markings and their effectiveness across the network path.
- Global Vantage Points (Agents):
    - Cloud Agents: A global network of pre-deployed monitoring agents located in major internet service provider (ISP) networks, public cloud regions, and metropolitan areas worldwide. These agents enable monitoring of external services and internet health from diverse global perspectives.
    - Enterprise Agents: Software agents deployed within an organization's own data centers, branch offices, or private cloud environments. These agents provide visibility into internal network performance and connectivity to external services.
    - Endpoint Agents: Lightweight agents installed on end-user devices (laptops, desktops). They provide real-time visibility into the user's local network conditions (Wi-Fi signal, VPN performance) and the application performance from their specific vantage point, crucial for remote and hybrid workforces.
- Digital Experience Monitoring:
    - Synthetic Monitoring: Runs proactive tests simulating user interactions with web applications, SaaS services (e.g., Microsoft 365, Salesforce, Webex, Zoom), and APIs. This helps detect issues before real users are impacted.
    - Real User Monitoring (Browser-based RUM): Collects performance data from actual user browser sessions, providing insights into load times, resource timing, and JavaScript errors from the end-user perspective (often integrated with AppDynamics).
- Internet Insights:
    - Collective Intelligence: Leverages aggregated data from billions of daily measurements across its global agent network to provide a macro-level view of internet health and detect widespread outages impacting ISPs, public clouds, and SaaS applications.
    - Outage Detection and Scope: Automatically identifies and scopes internet and application outages, providing immediate alerts and helping

IT teams understand if an issue is their responsibility or a third-party problem.

- Cloud Visibility (Cloud Insights):
    - Deep Cloud Network Path Details: Provides granular visibility into traffic paths within and between public cloud provider networks, including VPCs, availability zones, Direct Connect, and transit gateways.
    - Cloud Configuration Correlation: Correlates network performance with cloud infrastructure configuration changes, helping to identify if a configuration change led to a performance issue.
    - Cloud Inventory: Automatically inventories cloud resources and services impacting application delivery.
- Integrated Troubleshooting and Collaboration:
    - Shareable Test Data (ShareLinks): Allows easily sharing detailed network path visualizations and performance data with service providers or vendors to accelerate collaborative troubleshooting and prove where a fault lies.
    - Alerting and Notifications: Customizable alerts based on performance thresholds and anomaly detection.
- Integration with APM (e.g., Splunk AppDynamics):
    - Cross-Layer Correlation: Tightly integrates with APM solutions like Splunk AppDynamics to provide a holistic view that correlates application performance issues with underlying network and internet performance problems, enabling faster "mean time to innocence" (MTTI) and root cause analysis across the entire digital supply chain.

Collaboration Software

- Webex by Cisco

Collaboration Software

Webex by Cisco is a comprehensive collaboration platform that provides a unified suite of tools for meetings, messaging, calling, webinars, and events. It's designed to facilitate seamless communication and teamwork, particularly in today's increasingly hybrid work environments.

The core idea behind Webex is to offer "one place to message, call, meet, and share—with unparalleled security, integrated analytics, and the kind of intelligence only AI can deliver.":

Key Features of Webex by Cisco for Collaboration:

1. Meetings (Video Conferencing):

    - HD Video and Audio: High-definition video and crystal-clear audio ensure an immersive meeting experience.
    - Screen Sharing and Content Collaboration: Easily share your entire screen or specific applications. Integrated whiteboarding and annotation tools allow for real-time collaborative ideation.
    - Virtual Backgrounds and Noise Removal: Users can customize their backgrounds to maintain privacy or add professionalism. Advanced noise cancellation and voice optimization technology eliminate distracting background sounds (e.g., keyboard typing, barking dogs), ensuring everyone is heard clearly.
    - Recording and Transcription: Record meetings for later review, and get automatic, AI-powered transcriptions and summaries, making it easy to catch up or revisit key decisions.
    - Breakout Rooms and Polling: Divide participants into smaller groups for focused discussions. Conduct live polls and Q&A sessions to boost engagement and gather instant feedback.
    - Gesture Recognition: Uses AI to recognize hand gestures (e.g., thumbs up, clapping) and translate them into on-screen reactions, making virtual interactions more natural and expressive.
    - Immersive Share: Allows presenters to appear embedded within their shared content (e.g., presentation slides), creating a more engaging and personalized experience.
    - Meeting Lobbies and Host Controls: Securely admit participants from a waiting room, lock meetings, mute/unmute participants, and manage screen sharing permissions to maintain meeting integrity.
2. Messaging (Team Collaboration Spaces):

    - Persistent Group and 1:1 Chat: Create dedicated spaces for teams or projects for ongoing messaging, file sharing, and whiteboarding, keeping conversations organized and accessible.
    - File Sharing and Co-editing: Easily share files and collaborate on them directly within the messaging spaces.
    - Interactive Whiteboarding: Digital whiteboards for brainstorming and visual collaboration, with content saved within the space for later access.
    - Integration with Business Apps: Connects with popular third-party applications to streamline workflows and bring context into conversations.
3. Calling (Enterprise-Grade Cloud Calling):

    - Business Phone Number: Provides users with a business phone number for making and receiving calls.

    - Advanced Calling Features: Includes features like call forwarding, voicemail, visual voicemail, call transferring, and multi-way conference calling.
    - Device Flexibility: Make and receive calls on any device (desktop, mobile, Webex devices), with the ability to seamlessly move calls between devices.
    - AI-Powered Calling: Uses AI for features like proximity awareness and proactive pairing of users to devices.
4. Webinars and Events:

    - Large-Scale Event Hosting: Supports hosting of large-scale webinars and virtual events with interactive features, screen sharing, presentations, Q&A, and networking tools.
    - Hybrid Event Support: Tools for managing both in-person and virtual attendees, providing a consistent experience for hybrid events.
    - Registration and Ticketing: Built-in capabilities for event registration and ticketing management.
5. Artificial Intelligence (AI) Assistant:

    - Webex Assistant: A voice-activated assistant that can help with various tasks during meetings, such as starting recordings, taking notes, setting action items, and providing real-time highlights.
    - Real-time Translation and Transcription: Provides live closed captions and full transcriptions of meetings. Real-time translation from multiple spoken languages into over 100 captioned languages breaks down communication barriers.
    - Meeting Summaries: Generates concise summaries of meetings and message threads, making it easy to quickly grasp key points and decisions.
6. Intelligent Devices and Hardware Integration:

    - Wide Range of Devices: Cisco offers a full portfolio of Webex-optimized hardware, including video conferencing systems for rooms (Webex Room Series), personal desk devices (Webex Desk Series), cameras, headsets, and digital whiteboards.
    - Device Intelligence: These devices often feature AI-powered cameras (auto-framing, speaker tracking, people focus), noise cancellation, and seamless integration with the Webex software for enhanced experiences.
    - RoomOS: The operating system for Cisco's collaboration devices, providing a consistent, secure, and user-friendly experience.
7. Security and Compliance:

    - End-to-End Encryption: Offers strong encryption for communications

(meetings, messages, files) in transit and at rest, ensuring data privacy and security.
    - Meeting Lobbies and Access Controls: Features like meeting lobbies and granular host controls help prevent unauthorized access.
    - Identity Management: Supports Multi-Factor Authentication (MFA) and Single Sign-On (SSO) for secure user authentication.
    - Compliance: Complies with a wide range of global regulatory requirements, including GDPR, HIPAA, and ISO/IEC 27001.
8. IT Management and Analytics (Webex Control Hub):

    - Centralized Management: Provides a single, cloud-based pane of glass for IT administrators to provision users, manage devices, configure policies, and monitor service health across the entire Webex environment.
    - Analytics and Diagnostics: Offers deep insights into usage patterns, meeting quality, device performance, and user adoption, helping IT identify and resolve issues proactively.
    - Troubleshooting Tools: Built-in diagnostics and troubleshooting capabilities to quickly pinpoint and resolve collaboration problems.

How Webex by Cisco Supports Hybrid Work Environments:

Webex is specifically designed with hybrid work in mind, aiming to make collaboration inclusive, flexible, and secure regardless of where employees are working.

1. Flexibility and Location Agnosticism:

    - Consistent Experience: Provides a consistent user experience across different devices (desktop, mobile, room systems) and locations (home, office, on-the-go), enabling seamless transitions between work environments.
    - Any Device, Anywhere: Users can join meetings, send messages, and make calls from their preferred device and location, ensuring continuity of work.
2. Inclusivity in Meetings:

    - Equal Participation: AI-powered features like real-time translation, transcription, closed captioning, and optimize-for-all-voices ensure that all participants, regardless of language or location, can actively engage and understand discussions.
    - Smart Framing and Speaker Tracking: Webex devices with intelligent cameras ensure everyone in the physical room is clearly visible and that the active speaker is automatically framed, making remote participants feel more connected.

    - Noise Reduction: Eliminates background distractions from both ends of the call, improving focus and comprehension for all.
3. Enhanced Workspace Experiences (Office and Home):

    - Intelligent Room Devices: Cisco's Webex Room and Desk Series devices transform physical meeting spaces into highly collaborative, inclusive environments for hybrid teams, offering seamless integration with the Webex software.
    - "Bring Your Own Device" (BYOD) Support: Easy connectivity for personal laptops to room systems, allowing users to leverage the high-quality cameras and audio of the room.
    - Workspace Management Insights: Integrates with features for understanding room occupancy, environmental conditions, and meeting space utilization (often through Cisco DNA Spaces integration), helping organizations optimize office layouts for hybrid work.
4. Asynchronous Collaboration:

    - Video Messaging (Vidcast): Allows users to record and share short video messages and screen captures, enabling communication and collaboration even when team members are in different time zones or unable to meet live.
    - Persistent Messaging Spaces: Team spaces serve as a continuous hub for project information and discussions, reducing the need for live meetings for every update.
5. Security and Management for Distributed Teams:

    - Enterprise-Grade Security: Robust security features (encryption, access controls, compliance) provide peace of mind for IT administrators managing a distributed workforce.
    - Centralized IT Control (Control Hub): Provides IT with comprehensive visibility and management capabilities across all users, devices, and services, simplifying the oversight of a hybrid collaboration environment.
    - Network Integration: Integrates with Cisco's broader networking and security portfolio to ensure secure and optimized connectivity for remote workers and office locations.

Services (CX) Products

- Lifecycle Services
- Solution support
- Hardware support
- Software support
- Packaged services
- Solution consulting
- Cisco learning
- Customer stories
- View all Cisco services

Services (CX) Products

"Services (CX) Products" from Cisco refers to a broad portfolio of offerings designed to help customers maximize the value of their Cisco technology investments throughout their entire lifecycle. CX stands for Customer Experience, emphasizing a proactive, outcome-driven approach to ensure customer success and satisfaction. These services go beyond traditional break-fix support to include planning, adoption, optimization, and expert guidance.

1. Lifecycle Services

Cisco's Lifecycle Services are designed around a structured methodology to guide customers through every phase of their technology adoption, from initial planning to ongoing optimization. The widely known Cisco PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize) model is foundational to this approach.

- Prepare:
    - Business Alignment: Understanding customer's business objectives, pain points, and strategic goals.
    - High-Level Assessment: Initial analysis of current infrastructure and technical requirements to identify potential solutions.
- Plan:
    - Detailed Needs Analysis: In-depth assessment of technical, operational, and organizational readiness.
    - Project Planning: Defining project scope, timelines, resources, and success metrics.
    - Risk Assessment: Identifying and planning for potential project risks.
- Design:
    - Solution Architecture: Creating detailed network and solution designs that meet business and technical requirements.
    - Proof of Concept (PoC) / Lab Testing: Validating designs and functionalities in a controlled environment.
    - Security Integration: Ensuring security is built into the design from the ground up.
- Implement:

    - Deployment & Configuration: Installing and configuring hardware and software according to the design.
    - Migration Services: Assisting with seamless migration from old to new systems.
    - Integration: Integrating new solutions with existing IT infrastructure and applications.
    - User Acceptance Testing (UAT): Validating that the deployed solution meets user needs.
- Operate:
    - Monitoring & Management: Providing tools and expertise for ongoing network and solution monitoring, performance management, and fault detection.
    - Proactive Maintenance: Performing regular health checks and preventative maintenance to ensure uptime.
    - Incident Management: Swiftly responding to and resolving issues to minimize downtime.
    - Service Level Management: Ensuring that the solution meets defined service level agreements (SLAs).
- Optimize:
    - Performance Optimization: Continuously analyzing network and application performance to identify areas for improvement and efficiency gains.
    - Capacity Planning: Forecasting future resource needs and planning for scalability.
    - Security Posture Improvement: Regularly assessing and enhancing the security of the deployed solution.
    - Technology Adoption: Driving broader user adoption of new features and capabilities to maximize ROI.
    - Best Practices Implementation: Ensuring the solution is configured and operated according to Cisco and industry best practices.
    - Lifecycle Reviews: Regular reviews with customers to assess value realization, identify new opportunities, and plan for future evolution.

2. Solution Support

Cisco Solution Support is a specialized tier of technical support designed for complex, multi-product, and multi-vendor IT environments. It provides a centralized point of contact and accountability for resolving issues that span across Cisco products and third-party vendor solutions.

- Centralized Primary Point of Contact: Customers get a single point of contact (a designated Solution Support Engineer) for all eligible solution-level issues, regardless of whether the problem originates from Cisco or a third-party

product.

- Accountability and Continuity: The designated engineer manages the case from initial call to resolution, providing continuity and avoiding the need for customers to navigate multiple support organizations.
- Multi-Vendor Coordination: Cisco takes responsibility for coordinating with other solution vendors on the customer's behalf, streamlining troubleshooting and accelerating resolution for complex issues involving different technologies.
- Rapid Problem Resolution: Designed to accelerate problem diagnosis and resolution in intricate IT environments, minimizing downtime and business impact.
- Deep Solution Expertise: Access to highly skilled engineers who have deep knowledge of integrated Cisco and partner solutions, understanding how different components interact.
- Proactive Insights: Leverages insights from Cisco's knowledge base and experience with similar solution deployments to provide proactive recommendations and prevent recurring issues.
- 24/7 Access: Around-the-clock access to expert support via phone, web, and email.

3. Hardware Support (e.g., Cisco Smart Net Total Care)

Cisco Hardware Support services focus on maintaining the physical integrity and operational readiness of Cisco's vast array of hardware products.

- Technical Assistance Center (TAC) Access: 24/7 access to Cisco's global TAC, staffed by expert engineers who can provide troubleshooting assistance for hardware issues.
- Hardware Replacement: Fast and reliable hardware replacement options, with various service levels (e.g., Next Business Day (NBD), 4-hour, or 2-hour delivery) to minimize downtime.
- Onsite Field Engineer Option: For critical issues, the option to dispatch a field engineer to the customer's site for hardware replacement or repair.
- Device Diagnostics and Alerts: Automated tools and smart capabilities that can proactively monitor device health, detect potential failures, and generate alerts.
- Cisco.com Knowledge Base and Tools: Access to a comprehensive online repository of technical documentation, configuration guides, troubleshooting tools, and security advisories.
- Product Lifecycle Management: Provides insights into product end-of-life (EOL) and end-of-sale (EOS) dates to help with refresh planning.
- Service Coverage Management: Tools to track covered and uncovered products, assist with contract renewals, and budget planning.

4. Software Support (Cisco Software Support Service - SWSS)

Cisco Software Support Service (SWSS) ensures that Cisco software applications and licensed features perform optimally and remain up-to-date.

- Major, Minor, and Maintenance Releases: Access to all software updates, including new features, enhancements, security patches, and bug fixes, ensuring the software stays current and secure.
- Technical Assistance Center (TAC) Access: 24/7 access to Cisco TAC experts for software-related issues, providing troubleshooting and guidance.
- Online Support Resources: Access to Cisco's online knowledge base, documentation, forums, and interactive troubleshooting tools.
- License Management Support: Assistance with managing software licenses and ensuring compliance.
- Proactive Alerts: Notifications about software vulnerabilities, product advisories, and critical updates.
- API and Developer Support: For software-defined solutions, support for integrating with APIs and developing custom automations.

5. Packaged Services

Cisco Packaged Services are pre-defined, standardized service offerings designed for faster deployment, simplified ordering, and predictable outcomes for common technology implementations. They offer a structured approach to address specific customer needs.

- Standardized Scope: Clearly defined deliverables and activities for specific technology deployments or operational tasks (e.g., setting up a basic SD-WAN, implementing a wireless network, deploying collaboration endpoints).
- Accelerated Deployment: Designed for quick implementation, leveraging best practices and automation.
- Predictable Pricing and Outcomes: Transparent pricing and clear expectations for the results of the service.
- Reduced Complexity: Simplifies the process of acquiring and deploying services, particularly for smaller or less complex projects.
- Targeted Expertise: Delivered by Cisco experts or certified partners with specialized knowledge in the specific technology covered by the package.
- Examples: Could include services for quick start deployments, health checks, basic configurations, or specific feature enablement for a particular Cisco product (e.g., Webex Quick Start, DNA Center Basic Deployment).

6. Solution Consulting

Cisco Solution Consulting provides strategic and expert guidance to help organizations leverage Cisco technologies to achieve specific business outcomes and navigate complex IT challenges. It's about prescriptive advice and tailored roadmaps.

- Strategic Planning: Assisting organizations in developing IT strategies aligned with business goals, including digital transformation initiatives.
- Technology Advisory: Providing expert advice on technology selection, architecture design, and best practices for implementing Cisco solutions.
- Solution Architecture Design: Crafting detailed, customized solution architectures that integrate various Cisco products and potentially third-party technologies to meet unique business requirements.
- Assessment Services: Conducting in-depth assessments of current IT environments (network, security, cloud readiness, collaboration posture) to identify gaps, risks, and opportunities for improvement.
- Proof of Concept (PoC) & Pilot Guidance: Helping plan, execute, and evaluate PoCs and pilot programs for new technologies.
- Optimization Recommendations: Providing recommendations for optimizing existing Cisco deployments to improve performance, security, and efficiency.
- Hybrid Cloud Strategy: Guiding organizations on building and managing hybrid and multi-cloud environments effectively.
- Security Posture Development: Assisting with developing comprehensive security strategies, including Zero Trust, SASE, and OT security.
- Workforce Transformation: Consulting on how to leverage collaboration technologies to enable hybrid work and improve employee experience.
- Change Management: Advising on strategies to facilitate user adoption and manage the organizational impact of new technology deployments.

7. Cisco Learning

Cisco Learning offers a wide array of training and certification programs designed to educate IT professionals, developers, and network engineers on Cisco technologies. It aims to build and validate the skills needed to design, implement, operate, and optimize Cisco solutions.

- Certification Programs (e.g., CCNA, CCNP, CCIE): Industry-recognized certifications that validate expertise in various Cisco technologies (e.g., Enterprise Networking, Security, Data Center, Collaboration, DevNet).
- Training Courses: A comprehensive catalog of courses (instructor-led, online, self-paced, virtual labs) covering a broad range of Cisco products and technologies.
- Cisco U. (Digital Learning Platform): A personalized digital learning experience offering access to in-depth training, labs, and certification preparation for Cisco and Cisco-adjacent technologies.
- Cisco Networking Academy: A global education program that partners with academic institutions to provide networking and IT skills training to students.
- DevNet Learning: Resources specifically for developers, focusing on programmability, automation, and integrating with Cisco platforms via APIs.
- Hands-on Labs and Simulators: Provides access to virtual lab environments and

network simulators (like Cisco Modeling Labs) for practical, real-world experience.
- Continuing Education: Programs and resources to help certified professionals maintain and advance their certifications.
- Specialized Training: Courses focused on niche areas like cybersecurity, IoT, data center automation, and cloud networking.
- Custom Training Solutions: Tailored training programs for organizations with specific learning needs.

8. Customer Stories

Cisco leverages customer stories (case studies, testimonials, videos, webinars) to showcase how organizations have successfully implemented Cisco services and technologies to achieve tangible business outcomes.

- Real-World Examples: Provides concrete examples of how businesses have overcome challenges and achieved success using Cisco's products and services.
- Solution Validation: Demonstrates the effectiveness and value of Cisco's offerings in diverse industries and use cases.
- Business Outcome Focus: Highlights specific improvements in areas like operational efficiency, cost reduction, enhanced security, improved customer experience, and accelerated digital transformation.
- Inspiration and Best Practices: Offers insights and inspiration for prospective customers facing similar challenges.
- Credibility and Trust: Builds trust by demonstrating proven results and showcasing satisfied customers.
- Industry and Regional Relevance: Often categorized by industry, geography, or specific technology to make them relevant to different audiences.
- Diverse Formats: Available in various formats, including written case studies, video interviews, detailed reports, and presentations.

9. View All Cisco Services

This overarching category signifies the totality and breadth of Cisco's service offerings, emphasizing a holistic approach to customer success.

- Comprehensive Portfolio: Encompasses all the aforementioned service categories: technical support (hardware, software, solution), professional services (consulting, implementation), managed services, adoption services, and learning.
- Integrated Approach: Highlights how different services can be combined to provide end-to-end support throughout the customer lifecycle.
- Outcomes-Driven: Emphasizes Cisco's commitment to helping customers achieve their desired business outcomes, not just deploy technology.
- Flexibility and Customization: While some services are packaged, Cisco offers

flexibility to tailor service agreements to meet specific customer needs and complexities.
- Partner Ecosystem: Acknowledges the crucial role of Cisco's vast partner network in delivering these services, extending Cisco's reach and specialized expertise.
- Global Reach: Services are available globally, providing consistent support for multinational organizations.
- Digital Tools and Platforms: Leverages digital platforms (like Cisco Success Tracks, Cisco CX Cloud) to deliver insights, automation, and a unified experience for customers managing their services.

Featured Message

- Cisco Services: Make sure your technology delivers tangible business value with less risk and effort

featured message,

"Cisco Services: Make sure your technology delivers tangible business value with less risk and effort," encapsulates the core value proposition of Cisco's Customer Experience (CX) organization and its extensive portfolio of services.

"Make sure your technology delivers tangible business value..."

This part of the message highlights Cisco Services' commitment to moving beyond just providing technical support or deploying products. It emphasizes an outcome-driven approach.

- Tangible Business Value: This refers to quantifiable and measurable benefits that directly impact an organization's bottom line or strategic objectives. This could include:
    - Increased Revenue: Through faster time to market for new services, improved customer experience, or enhanced operational efficiency.
    - Reduced Costs: By optimizing IT operations, consolidating infrastructure, or preventing costly downtime.
    - Improved Efficiency/Productivity: Through streamlined workflows, enhanced collaboration, or automated processes.
    - Enhanced Security Posture: Minimizing breaches, protecting sensitive data, and ensuring compliance.
    - Better Customer Experience: Ensuring applications and services are always available and performant.
    - Faster Innovation: Enabling IT to be a strategic partner rather than just a cost center.
- Beyond "speeds and feeds": Cisco acknowledges that simply purchasing

advanced technology isn't enough. The real value comes from its effective implementation, adoption, and ongoing optimization, which services facilitate.

"...with less risk..."

This part of the message addresses the inherent challenges and potential pitfalls associated with complex technology deployments and ongoing operations. Cisco Services aim to mitigate these risks significantly.

- Reduced Deployment Risk:
    - Expert Planning & Design: Services like Solution Consulting and Lifecycle Services (Prepare, Plan, Design phases) ensure that solutions are correctly designed and sized for specific needs, avoiding costly reworks or performance issues.
    - Proven Methodologies: Leveraging established best practices (like PPDIOO) and experienced professionals reduces the likelihood of project delays, budget overruns, or technical failures.
    - Pre-tested Solutions: For complex integrated solutions, services ensure components work together seamlessly, minimizing unforeseen compatibility issues.
- Reduced Operational Risk:
    - Proactive Monitoring & Maintenance: Services like Managed Services and Hardware/Software Support detect and address potential issues before they cause outages, reducing unplanned downtime.
    - Rapid Problem Resolution: Solution Support provides a single point of contact for complex issues, accelerating diagnosis and resolution across multi-vendor environments.
    - Security Expertise: Services help implement and maintain robust security postures, reducing the risk of cyberattacks and data breaches.
    - Compliance Adherence: Guidance and support to ensure technology deployments meet industry and regulatory compliance requirements.
- Reduced Adoption Risk:
    - Training & Enablement: Cisco Learning and Adoption Services ensure that users and IT staff are proficient with new technologies, maximizing their utilization and preventing under-adoption.
- Reduced Financial Risk:
    - Optimized Investment: Ensuring technology delivers its full potential means better ROI.
    - Predictable Costs: Packaged services and structured support contracts offer predictable operational expenses.

"...and effort."

This aspect of the message speaks directly to the operational burden on IT teams. Cisco Services are designed to lighten this load, freeing up internal resources.

- Simplified Operations:
    - Centralized Management: Services complement platforms like Cisco Intersight and Catalyst Center, which consolidate management, reducing the number of tools and interfaces IT needs to learn and manage.
    - Automation: Services help customers leverage automation capabilities inherent in Cisco products, reducing manual, repetitive tasks.
    - Expert Assistance: Offloading complex tasks (e.g., advanced troubleshooting, specialized configurations, security hardening) to Cisco experts allows internal teams to focus on core business initiatives.
- Accelerated Deployment & Time to Value:
    - Faster Implementations: Services like Packaged Services and Implementation Services streamline deployments, bringing new capabilities online more quickly.
    - Reduced Learning Curve: Training services empower teams faster.
- Streamlined Support:
    - Single Point of Contact: Solution Support simplifies the troubleshooting process by removing the need for customers to coordinate with multiple vendors.
    - Proactive Care: Minimizes reactive firefighting, allowing IT to be more strategic.
- Resource Optimization:
    - Augmenting Staff: Services can fill skill gaps or augment existing IT teams, allowing organizations to achieve more without increasing headcount.

In Summary:

The "Featured Message" acts as a concise summary of Cisco's Customer Experience (CX) value proposition:

- Focus on Outcomes: It's not just about selling boxes; it's about helping customers succeed with their technology.
- Risk Mitigation: Addressing the inherent complexities and potential pitfalls of modern IT.
- Operational Efficiency: Simplifying IT management and freeing up valuable internal resources.

Solutions Section

Main Solution Categories

1. Industries - Industry-specific solutions
2. Technologies - Technology-focused solutions
3. Service Providers - Solutions for service provider market
4. Small and Medium Business - SMB-focused solutions

Main Solution Categories

These are the primary ways a company organizes its offerings to help customers quickly find what they're looking for based on their specific context or focus.

1 Industries - Industry-specific solutions

This category highlights how a vendor's technology and services are tailored to meet the unique challenges, regulatory requirements, and operational needs of specific vertical markets. Instead of selling generic products, the vendor positions itself as a strategic partner that understands the nuances of a particular industry.

Key Features/Characteristics:

- Tailored Use Cases: Demonstrates how their products solve problems specific to an industry (e.g., connected factories for manufacturing, telehealth for healthcare, smart campuses for education).
- Compliance & Regulatory Expertise: Addresses industry-specific regulations (e.g., HIPAA for healthcare, PCI DSS for retail, NERC-CIP for energy/utilities).
- Vertical-Specific Language & Messaging: Uses terminology and speaks to the pain points relevant to that industry's professionals (e.g., "patient care" instead of just "network uptime" for healthcare).
- Integrated Solutions: Often combines multiple technologies (e.g., IoT, cybersecurity, collaboration, data analytics) into a cohesive solution package for a specific industry.
- Examples of Industries:
    - Healthcare: Digital health, telehealth, secure patient data, clinical collaboration.
    - Manufacturing: Industrial IoT, predictive maintenance, operational technology (OT) security, smart factory automation.
    - Retail: Omnichannel experience, personalized shopping, in-store analytics, secure POS systems.
    - Education: Hybrid learning environments, campus networking, student safety, remote access.
    - Financial Services: Secure transactions, fraud detection, digital banking, regulatory compliance.
    - Government: Secure public safety networks, smart city initiatives, critical infrastructure protection.
- Why it Matters: Customers in specific industries prefer vendors who demonstrate a deep understanding of their unique business environment, rather than just offering generic technology.

2 Technologies - Technology-focused solutions

This category focuses on how specific core technologies (like networking, cybersecurity, cloud, or AI) are applied to solve a broad range of problems across various industries. It targets buyers who are primarily interested in a particular technological domain or who are building their infrastructure around certain tech stacks.

Key Features/Characteristics:

- Deep Dive into Specific Tech: Explains the capabilities and benefits of a particular technology (e.g., what SD-WAN can do, how AI/ML enhances operations, the advantages of a unified communications platform).
- Platform-Centric: Often highlights a core platform or product family as the foundation for various solutions (e.g., Cisco's enterprise networking portfolio, their security suite, their data center offerings).
- Broad Applicability: Shows how the technology can be used in diverse scenarios, not limited to one industry.
- Focus on Technical Capabilities: Emphasizes features, performance, scalability, and integration aspects of the technology itself.
- Examples of Technologies:
    - Networking: Enterprise networking (LAN, WLAN), SD-WAN, data center networking, cloud networking.
    - Cybersecurity: Network security, endpoint security, cloud security, identity and access management, threat intelligence.
    - Cloud: Hybrid cloud, multi-cloud management, cloud native development.
    - Collaboration: Unified communications, video conferencing, team messaging.
    - IoT: IoT connectivity, IoT security, edge computing.
    - Observability: APM, network visibility, logging, tracing.
    - Automation: Network automation, IT automation.
- Why it Matters: IT professionals, architects, and technical decision-makers often start their search based on the specific technology they need to implement or upgrade.

3 Service Providers - Solutions for service provider market

This category specifically targets telecommunications companies, managed service providers (MSPs), internet service providers (ISPs), and other organizations that deliver network and IT services to their own customers. The solutions are designed to help service providers build, operate, and monetize their networks and service offerings.

Key Features/Characteristics:

- Network Infrastructure for Carriers: Solutions for core routing, optical

networking, access networks (5G, fiber, cable), and aggregation.
- Cloud and Data Center for Service Providers: Platforms and infrastructure for building cloud services, colocation, and managed data center offerings for their clients.
- Service Orchestration and Automation: Tools to automate the provisioning, management, and assurance of customer services across complex provider networks.
- Software-Defined Networking (SDN) & Network Function Virtualization (NFV): Solutions for virtualizing network functions and building highly agile and programmable networks.
- Security for Service Provider Infrastructure: Protecting their own vast networks and providing security services to their subscribers.
- Monetization & New Services: Helping service providers launch new revenue-generating services (e.g., managed SD-WAN, managed security, IoT connectivity, enterprise cloud services).
- Scale and Performance: Solutions built to handle the massive scale, high performance, and extreme reliability requirements of carrier-grade networks.
- Operational Efficiency (OpEx Reduction): Tools and architectures that help service providers reduce their operational costs.
- Examples: Solutions for 5G network transformation, broadband access, enterprise managed services, IoT service platforms, web-scale networking.
- Why it Matters: Service providers have very distinct needs from enterprises, focusing on massive scale, multi-tenancy, highly reliable infrastructure, and the ability to provision and bill for services.

4 Small and Medium Business (SMB) - SMB-focused solutions

This category addresses the specific needs of small and medium-sized businesses, which often have limited IT budgets, fewer dedicated IT staff, and different scalability requirements compared to large enterprises. The focus is on simplicity, affordability, and ease of management.

Key Features/Characteristics:

- Simplicity and Ease of Use: Solutions that are easy to deploy, configure, and manage, often cloud-managed, minimizing the need for specialized IT expertise.
- Cost-Effectiveness: Pricing models and product features tailored to SMB budgets, often with subscription-based services.
- All-in-One Solutions: Often combines multiple functionalities into a single device or platform (e.g., a security appliance with built-in Wi-Fi and routing).
- Scalability for Growth: Solutions that can easily scale as the business grows, without requiring a complete overhaul.
- Essential Security: Provides foundational security capabilities to protect against common threats without overwhelming complexity.

- Reliability and Uptime: Ensures business continuity with reliable network connectivity and data protection.
- Focus on Core Business Needs: Solutions that directly address common SMB challenges like reliable internet access, secure remote work, basic collaboration, and data backup.
- Examples: Cloud-managed Wi-Fi and security appliances (like Cisco Meraki Go or some Meraki MX/MR/MS models), simplified collaboration tools, entry-level network switches, basic cybersecurity bundles.
- Why it Matters: SMBs look for solutions that are practical, affordable, and require minimal IT overhead, allowing them to focus on their core business rather than complex IT management.

By Industry (13+ Verticals)

- Cities and Communities
- Education
- Financial Services
- Government
- Healthcare
- Manufacturing
- Mining
- Oil and and Gas
- Retail
- Smart Buildings
- Sports, Media, and Entertainment
- Transportation
- Utilities
- View all industries

By Industry (13+ Verticals)

1. Cities and Communities (Smart Cities)

- Challenges: Urbanization, sustainability, public safety, efficient resource management, digital divide, aging infrastructure, traffic congestion.
- Cisco Solutions Focus:
    - Smart Infrastructure: Connected streetlights (PoE-powered), smart parking, environmental monitoring (air quality sensors).
    - Public Safety: Video surveillance with analytics, secure communication for first responders, emergency services.

    - Public Wi-Fi: Bridging the digital divide and enabling connectivity for citizens and IoT devices.
    - Transportation Management: Intelligent traffic systems, connected transit (buses, trains), smart intersections.
    - Government Services: Digital citizen engagement, secure e-government platforms, data-driven urban planning.
    - Resilience: Building robust, secure, and adaptable urban infrastructure.

2. Education

- Challenges: Hybrid learning (remote and in-person), student and data security, campus network performance, digital divide, remote teaching tools, budget constraints.
- Cisco Solutions Focus:
    - Hybrid Learning: Webex for virtual classrooms, collaboration devices for interactive teaching, secure remote access for students and faculty.
    - Campus Networking: High-performance wired and wireless (Wi-Fi 6/7) networks for high-density environments, secure segmentation for different user groups (students, faculty, guests).
    - Cybersecurity: Protecting student and faculty data (FERPA/COPPA compliance), ransomware protection, secure endpoints, identity management.
    - Physical Security: IP-based surveillance systems for campus safety.
    - Cisco Networking Academy: Training and certification programs for future IT professionals and upskilling educators.

3. Financial Services

- Challenges: Cybersecurity threats (fraud, data breaches), regulatory compliance (PCI DSS, GDPR), digital transformation (online banking, mobile payments), customer experience, branch modernization, secure remote work.
- Cisco Solutions Focus:
    - Advanced Security: Threat detection and prevention, data loss prevention (DLP), secure network segmentation, Zero Trust, multi-factor authentication (MFA) for protecting sensitive financial data and transactions.
    - Secure Collaboration: Webex for secure client interactions (tele-banking), internal team collaboration across branches, and remote advisor access.
    - Branch Transformation: SD-WAN for optimized and secure connectivity to cloud applications, cloud-managed IT (Meraki) for simplified branch deployments.
    - Data Center Modernization: High-performance, secure, and compliant

infrastructure for core banking applications and analytics.
    - Customer Experience: Enhancing digital channels and in-branch experiences through connected technologies.

4. Government

- Challenges: Data security and privacy, regulatory compliance (FedRAMP, CMMC), secure remote work for public sector employees, aging infrastructure, inter-agency collaboration, citizen engagement, budget constraints.
- Cisco Solutions Focus:
    - Secure Collaboration: FedRAMP-authorized Webex for secure meetings, messaging, and calling, enabling efficient inter-agency and remote work.
    - Cybersecurity: Robust threat detection, prevention, and response capabilities, secure network segmentation, identity management, and compliance solutions.
    - Critical Infrastructure Protection: Securing operational technology (OT) and critical control systems.
    - Network Modernization: Building scalable, secure, and resilient networks for federal, state, and local government operations.
    - Smart Government Initiatives: Leveraging IoT and data analytics for more efficient public services.

5. Healthcare

- Challenges: Cybersecurity (ransomware, data breaches of PHI), telehealth and virtual care delivery, real-time data access, secure IoT medical devices, interoperability, regulatory compliance (HIPAA), clinical collaboration.
- Cisco Solutions Focus:
    - Telehealth & Virtual Care: Webex for secure virtual consultations, remote patient monitoring, and virtual rounding, often integrating with EHR systems.
    - Cybersecurity: Protecting patient data (PHI), network segmentation for medical devices, threat detection, and secure access for clinicians.
    - Clinical Collaboration: Secure messaging and real-time communication tools for care teams.
    - Connected Healthcare: Securely connecting medical IoT devices (IoMT) for real-time data, asset tracking, and improved patient care.
    - High-Performance Networks: Reliable and secure wired and wireless networks for critical hospital operations and data transfer.

6. Manufacturing

- Challenges: Industry 4.0 adoption, OT/IT convergence, cybersecurity for industrial control systems, supply chain visibility, predictive maintenance, operational efficiency, worker safety.
- Cisco Solutions Focus:
    - Industrial IoT (IIoT): Securely connecting machines, sensors, and devices on the factory floor for real-time data collection and analysis.
    - OT Security (Cisco Cyber Vision): Deep visibility and threat detection for industrial control systems, enabling secure IT/OT convergence.
    - Network for Industry 4.0: Resilient, high-performance industrial networking (wired and wireless) to support automation, robotics, and edge computing.
    - Predictive Maintenance: Using IoT data and analytics to anticipate equipment failures and reduce downtime.
    - Worker Collaboration: Secure collaboration tools for factory floor workers and remote experts.
    - Supply Chain Optimization: Providing visibility and secure connectivity across the entire supply chain.

7. Mining

- Challenges: Remote and harsh operating environments, worker safety, autonomous operations (vehicles, drills), real-time data collection, reliable communication, cybersecurity for OT systems, environmental monitoring.
- Cisco Solutions Focus:
    - Ruggedized Networking: Industrial-grade networking equipment (switches, routers, wireless access points) designed for extreme conditions.
    - Wireless Connectivity: Robust and reliable wireless (Wi-Fi, 5G/LTE private networks) for autonomous vehicles, remote operations, and worker communications.
    - IoT for Mining: Connecting sensors and equipment for telemetry, condition monitoring, and predictive maintenance.
    - OT Security: Protecting critical mining infrastructure and control systems from cyber threats.
    - Integrated Operations Centers (iROCs): Solutions for centralizing monitoring and control of distributed mining operations.
    - Worker Safety: Connected worker solutions, video surveillance, and emergency communication systems.

8. Oil and Gas

- Challenges: Remote and distributed operations (drilling sites, pipelines), extreme

environments, cybersecurity for critical infrastructure, data collection from sensors, regulatory compliance, operational efficiency, worker safety.

- Cisco Solutions Focus:
    - Industrial IoT: Connecting sensors on wells, pipelines, and refineries for real-time monitoring and control.
    - OT Security: Securing SCADA systems, control networks, and operational data.
    - Ruggedized & Resilient Networks: Building highly reliable and secure networks for onshore, offshore, and pipeline operations.
    - Remote Operations: Secure remote access for engineers and technicians to field equipment.
    - Predictive Maintenance: Using data analytics to optimize equipment performance and prevent failures.
    - Environmental Monitoring: Leveraging sensors for compliance and safety.

9. Retail

- Challenges: Enhancing in-store customer experience, omnichannel integration, inventory management, physical security, payment security (PCI compliance), workforce productivity, branch connectivity.
- Cisco Solutions Focus:
    - In-Store Experience: High-performance Wi-Fi for customers and associates, personalized offers via location analytics, digital signage.
    - Omnichannel Support: Integrating online and in-store operations with secure and reliable connectivity.
    - Physical and Cyber Security: IP cameras (Meraki MV), secure POS systems, advanced threat protection, segmentation for guest Wi-Fi and critical systems.
    - Store Operations: SD-WAN for optimized branch connectivity, cloud-managed IT (Meraki) for simplified management of distributed stores.
    - Workforce Collaboration: Tools to empower associates with real-time inventory and customer information.

10. Smart Buildings

- Challenges: Energy efficiency, occupant comfort and experience, building automation integration, physical security, sustainability, operational cost reduction, hybrid workspace management.
- Cisco Solutions Focus:
    - Converged IP Network: A single, secure IP network backbone for all

building systems (HVAC, lighting, security, access control), leveraging Power over Ethernet (PoE) for simplified cabling and power.
    - IoT Integration: Connecting smart sensors and devices for real-time data on occupancy, temperature, air quality, and lighting.
    - Building Automation Systems (BAS) Integration: Seamlessly integrating disparate building systems for centralized control and automation.
    - Physical Security: IP video surveillance, access control, and alarm systems.
    - Workspace Optimization: Using analytics (Cisco Spaces) to understand building utilization, optimize space, and enhance occupant experience.
    - Sustainability: Reducing energy consumption through intelligent control of lighting and HVAC.

11. Sports, Media, and Entertainment

- Challenges: High-density Wi-Fi for fans, delivering immersive experiences (4K/8K video), live broadcast production, cybersecurity for intellectual property, event security, guest services.
- Cisco Solutions Focus:
    - High-Density Wi-Fi (Wi-Fi 7): Providing robust, high-performance wireless connectivity for thousands of concurrent users in stadiums, arenas, and event venues.
    - IP Fabric for Media (IPFM): High-bandwidth, low-latency IP networks for real-time, uncompressed video production and distribution (4K, 8K, HDR).
    - Digital Signage & IPTV: Delivering dynamic content and advertising throughout venues (e.g., Wipro VisionEDGE integrated with Cisco).
    - Fan Engagement: Location-based services, mobile apps, and personalized content delivery.
    - Event Security: IP surveillance, access control, and secure communication for event staff.
    - Hybrid Work for Production: Secure collaboration for distributed media teams.

12. Transportation

- Challenges: Connected roadways and vehicles, public transit efficiency, physical security for infrastructure (airports, ports, rail), passenger experience, traffic management, IoT for asset tracking.
- Cisco Solutions Focus:
    - Intelligent Transportation Systems (ITS): Connected roadways, smart intersections, and traffic flow optimization.

    - Connected Transit: Secure and reliable networks for trains, buses, and subways, enhancing operational efficiency and passenger connectivity.
    - Airport Solutions: Improving passenger flow, baggage handling, operational efficiency, and security within airports.
    - Port and Terminal Modernization: Automating operations, enhancing security, and optimizing logistics.
    - IoT for Transportation: Asset tracking (vehicles, containers), predictive maintenance for infrastructure, and environmental monitoring.
    - Cybersecurity: Protecting critical transportation infrastructure from cyber threats.

13. Utilities

- Challenges: Grid modernization (smart grid), cybersecurity for critical infrastructure (SCADA, OT), remote asset monitoring, regulatory compliance, operational efficiency, renewable energy integration.
- Cisco Solutions Focus:
    - Smart Grid Infrastructure: Secure and reliable communication networks for smart meters, substations, and distributed energy resources.
    - OT Security: Protecting operational technology and industrial control systems (SCADA) from cyberattacks.
    - Remote Asset Monitoring: IoT solutions for monitoring pipelines, power lines, and other distributed assets.
    - Field Area Networks (FAN): Secure and resilient wireless communication for utility workers and remote equipment.
    - Data Analytics: Using data from the grid for predictive maintenance, demand forecasting, and optimized energy distribution.
    - Compliance: Solutions to help meet industry-specific regulations for critical infrastructure.

Featured Tool

- Portfolio Explorer: Build the bridge between business outcomes and technology with our new interactive tool

The "Featured Tool: Portfolio Explorer" is a strategic interactive tool that Cisco offers to help organizations bridge the gap between their high-level business objectives and the underlying technology solutions required to achieve them.

It serves as a guide for customers (and potentially Cisco's sales teams and partners) to navigate Cisco's vast product and services portfolio in a way that is relevant to their

specific business context.

Purpose of Cisco Portfolio Explorer

The primary purpose of the Portfolio Explorer is to:

1. Translate Business Outcomes into Technology Solutions: Instead of starting with "What product do I need?", it starts with "What business problem am I trying to solve?" or "What outcome do I want to achieve?". It then maps those outcomes to relevant Cisco technologies, products, and services.
2. Simplify Portfolio Navigation: Cisco has an incredibly broad and deep portfolio. The Portfolio Explorer helps customers (especially those not deeply familiar with every Cisco product) quickly identify the relevant parts of that portfolio for their specific needs.
3. Demonstrate Value and Relevance: It helps Cisco illustrate how its diverse offerings work together to create integrated solutions that deliver tangible value in real-world scenarios.
4. Educate and Guide: It acts as an educational resource, providing insights into common industry themes, use cases, and the technologies that underpin them.

How it Builds the Bridge Between Business Outcomes and Technology

The Portfolio Explorer typically works by:

- Starting with Business Themes/Outcomes: Users can select high-level business goals or strategic initiatives relevant to their organization or industry. Examples could include:
    - "Enhance Customer Experience"
    - "Improve Operational Efficiency"
    - "Strengthen Cybersecurity Posture"
    - "Enable Hybrid Work"
    - "Drive Digital Transformation"
    - "Achieve Sustainability Goals"
- Drilling Down to Use Cases: Once a business outcome is selected, the tool likely presents specific, actionable "use cases" that contribute to that outcome. For example, under "Improve Operational Efficiency," a use case might be "Automate Network Provisioning" or "Implement Predictive Maintenance for Industrial Assets."
- Mapping to Cisco Technologies and Solutions: For each use case, the Portfolio Explorer then identifies the specific Cisco products, software, services, and architectures that enable it. This could involve:
    - Networking Hardware: (e.g., Catalyst switches, Meraki access points)
    - Software: (e.g., Cisco DNA Center, AppDynamics, SecureX, Webex)
    - Security Solutions: (e.g., Secure Firewall, Duo, Umbrella)
    - Services: (e.g., Solution Consulting, Lifecycle Services, Software Support)

    - Architectural Frameworks: (e.g., Zero Trust, SASE, SD-WAN)
- Providing Context and Resources: The tool often includes:
    - Descriptions: Explanations of how the technology supports the use case.
    - Success Stories/Case Studies: Links to real-world examples of other customers who achieved similar outcomes using these solutions.
    - Technical Overviews: Deeper dives into the technical components if desired.
    - Partnerships: Information on how Cisco's ecosystem partners contribute to the solution.

Benefits of Using the Portfolio Explorer

1. For Customers:
    - Faster Solution Discovery: Quickly identifies relevant solutions without having to browse countless individual product pages.
    - Clearer Value Proposition: Helps them understand the "why" behind technology investments – how they lead to concrete business results.
    - Improved Decision-Making: Provides a structured way to consider solutions based on strategic objectives, not just technical specifications.
    - Better Communication: Enables IT leaders to better articulate the business value of technology investments to executive stakeholders.
    - Reduced Risk: By showing proven pathways to desired outcomes, it helps de-risk technology projects.
2. For Cisco (Sales & Marketing):
    - Outcome-Based Selling: Shifts conversations from product features to business value.
    - Sales Enablement: Provides a powerful tool for sales teams to guide customer discussions and demonstrate solution relevance.
    - Lead Generation: Attracts customers who are looking for solutions to business problems, not just individual products.
    - Market Differentiation: Highlights Cisco's ability to deliver integrated, outcome-oriented solutions rather than fragmented point products.

By Technology (5 Main Categories)

- Artificial Intelligence
    - AI-enabled network operations
    - Cisco AI
    - Cisco AI Assistant
    - Mass-scale AI infrastructure

By Technology: Artificial Intelligence

Artificial Intelligence (AI) at Cisco is about leveraging machine learning (ML), deep learning (DL), natural language processing (NLP), and other AI techniques to make networks smarter, security more proactive, collaboration more intuitive, and operations more automated.

1. AI-enabled network operations (AIOps)

This refers to the application of AI and Machine Learning (ML) to automate and enhance network operations. The goal is to move from reactive troubleshooting to proactive and even predictive network management.

- Key Features/Benefits:
    - Proactive Issue Detection & Prevention: AI algorithms analyze vast amounts of network data (logs, metrics, traces, events) in real-time to identify patterns, anomalies, and potential issues *before* they impact users or services. This moves beyond traditional threshold-based alerts.
    - Automated Root Cause Analysis: By correlating data across various network domains (wired, wireless, WAN, data center, cloud), AI helps pinpoint the exact cause of a problem much faster than manual methods.
    - Predictive Maintenance: Forecasting network component failures or performance degradations based on historical data and current trends.
    - Network Optimization: Dynamically adjusting network configurations, traffic routing, and resource allocation to ensure optimal performance, especially for critical applications (e.g., automatically shifting bandwidth for a Webex call).
    - Reduced Operational Costs: Automating routine tasks (troubleshooting, configuration, monitoring) and reducing human error.
    - Enhanced Security: Identifying unusual network behaviors that might indicate a security threat, beyond signature-based detection.
    - Simplified Troubleshooting: Providing actionable insights and recommended actions to IT teams, reducing Mean Time To Resolution (MTTR).
- Cisco Examples: Cisco DNA Center (now Cisco Catalyst Center) and Cisco Meraki both heavily leverage AI/ML for network assurance, intelligent analytics, automated provisioning, and proactive issue resolution in wired, wireless, and SD-WAN environments. Cisco Nexus Dashboard Insights uses AI/ML for data center network analytics.

2. Cisco AI

This likely represents Cisco's overarching strategy and platform for integrating AI across its entire product portfolio. It's the "umbrella" under which all other AI initiatives fall.

- Key Aspects:
    - Responsible AI Framework: Cisco emphasizes a commitment to ethical AI development, focusing on data privacy, transparency, and security.
    - Unified AI Platform: Building a consistent AI foundation and capabilities that can be shared and integrated across different product lines (networking, security, collaboration, contact center).
    - Strategic Partnerships: Collaborating with AI leaders (e.g., NVIDIA) to leverage specialized AI hardware and software for optimal performance.
    - Focus on Business Outcomes: Ensuring that AI deployments deliver measurable improvements in efficiency, security, customer experience, and innovation.
    - AI for Cisco's Own Operations: Using AI to improve Cisco's internal supply chain, customer support, and R&D processes.

3. Cisco AI Assistant

This refers to specific AI-powered virtual assistants or intelligent interfaces embedded within Cisco products to simplify operations and enhance user experience. These assistants often leverage generative AI and natural language processing (NLP).

- Key Features/Benefits:
    - Conversational Interfaces: Users can interact with the AI assistant using natural language queries to get information, perform tasks, or troubleshoot issues.
    - Contextual Guidance: Provides relevant information and recommendations based on the user's current context within the application or device.
    - Automated Tasks: Can automate simple configuration changes, data retrieval, or report generation.
    - Troubleshooting Assistance: Guides users through troubleshooting steps or provides explanations for alerts and errors.
    - Summarization & Transcription: In collaboration tools, automatically transcribing meetings, generating summaries, and identifying action items.
- Cisco Examples:
    - Webex AI Assistant: Embedded in Webex meetings for real-time transcription, translation, intelligent summaries, and action item generation. Also in Webex Contact Center to assist agents and supervisors with real-time customer insights, suggested responses, and call summaries.
    - Cisco Secure Firewall AI Assistant: Helps administrators manage firewall policies, create rules, and troubleshoot issues by answering questions about configurations and providing contextual guidance.

4. Mass-scale AI infrastructure

This category focuses on the underlying hardware, software, and networking infrastructure required to support large-scale AI training, inference, and data processing. AI workloads are incredibly compute and data-intensive, demanding highly specialized and performant infrastructure.

- Key Components/Characteristics:
    - High-Performance Compute (HPC): Utilizing specialized processors like GPUs (Graphics Processing Units), TPUs (Tensor Processing Units), and AI Accelerators, which are optimized for parallel processing required by AI/ML algorithms. Cisco offers AI-optimized servers (e.g., UCS X-Series with NVIDIA GPUs).
    - High-Bandwidth, Low-Latency Networking: Crucial for efficient data transfer between compute nodes, storage, and data sources. This involves high-speed Ethernet (e.g., Cisco Nexus Hyperfabric AI, Silicon One), InfiniBand, and specialized AI network fabrics.
    - Scalable Storage Solutions: Designed to handle vast datasets required for AI model training, including data lakes, distributed file systems, and high-performance storage.
    - Optimized Software Stacks: Integrating with AI/ML frameworks (TensorFlow, PyTorch), MLOps platforms (for managing the AI lifecycle), and orchestration tools.
    - Validated Designs (Cisco AI PODs): Pre-configured, integrated, and tested bundles of compute, storage, and networking tailored for specific AI workloads, simplifying deployment and ensuring optimal performance.
    - Sustainability: Designing energy-efficient infrastructure to handle the significant power demands of AI.
- Cisco's Role: Cisco provides the critical networking backbone for AI data centers and clusters, as well as AI-optimized compute platforms (UCS servers) and validated architectures (AI PODs, Nexus Hyperfabric AI) that integrate with leading AI hardware and software partners (e.g., NVIDIA). Their focus is on building the "AI-native infrastructure" that can securely and efficiently power AI workloads at scale.

- Networking
    - Cloud and data center networking
    - Cloud-managed networking (Meraki)
    - Industrial IoT
    - SD-WAN
    - Smart buildings
    - All networking solutions

Networking

1. Cloud and Data Center Networking

This category encompasses solutions for building, managing, and connecting modern data centers and extending connectivity to various cloud environments (public, private, hybrid). The focus is on agility, automation, security, and performance for critical applications and data.

- Key Features:
    - Software-Defined Networking (SDN) with Cisco ACI (Application Centric Infrastructure): A policy-driven automation framework that abstracts network complexity, allowing IT to define application requirements and have the network automatically configure itself to meet those needs. It provides centralized control, real-time visibility, and simplifies network operations.
    - Cisco Nexus Switches: High-performance, low-latency switches designed for data center environments, supporting a wide range of protocols, virtualization, and advanced features for scale and agility.
    - Cisco Unified Computing System (UCS): An integrated, converged infrastructure platform that combines computing, networking, storage access, and virtualization into a single system, simplifying data center management and improving performance.
    - Cloud Interconnect/Cloud OnRamp: Secure and optimized connectivity to public cloud providers (AWS, Azure, GCP) for hybrid cloud architectures, ensuring consistent policy enforcement and performance.
    - Hyperconverged Infrastructure (HCI) with Cisco HyperFlex: Combines compute, storage, and networking into a single, easy-to-manage platform, simplifying deployment and scaling of virtualized environments.
    - Network Automation & Orchestration: Tools and APIs for automating network provisioning, configuration, and troubleshooting, often integrated with Cisco Intersight (a cloud-based management platform).
    - Microsegmentation: Granular security policies that isolate workloads within the data center or cloud, limiting the lateral movement of threats.
    - Visibility and Analytics: Provides deep insights into application performance, network traffic, and resource utilization for proactive monitoring and troubleshooting.

2. Cloud-Managed Networking (Meraki)

Cisco Meraki offers a distinctive approach to networking where the entire network infrastructure (wireless, switching, security, SD-WAN, and even smart cameras) is

centrally managed from a cloud-based dashboard. This simplifies deployment and operations, making it ideal for distributed environments, branches, and organizations with limited IT staff.

- Key Features:
    - 100% Cloud-Managed Dashboard: A single, intuitive web-based interface for configuring, monitoring, and troubleshooting all Meraki devices globally, eliminating the need for on-premises controllers.
    - Zero-Touch Provisioning: Devices self-provision upon connection to the internet, allowing for rapid deployment in remote locations without requiring on-site IT expertise.
    - Unified Management: Integrates Wi-Fi (access points), switching, security appliances (firewalls/routers/SD-WAN), and smart cameras onto one platform.
    - Layer 7 Visibility and Control: Provides deep insight into application usage, allowing for granular traffic shaping, bandwidth limits, and content filtering.
    - Integrated Security: Built-in security features like firewalls, intrusion prevention (IPS), content filtering, and auto-VPN for secure site-to-site connectivity.
    - Location Analytics (CMX): Leveraging Wi-Fi data to provide insights into foot traffic, dwell times, and user behavior in physical spaces.
    - Scalability without Complexity: Designed to scale from small businesses to large, distributed enterprises with tens of thousands of devices, all managed from the same dashboard.
    - Automatic Firmware Updates: Ensures devices are always running the latest software and security patches without manual intervention.

3. Industrial IoT (IIoT)

Cisco's Industrial IoT networking solutions are purpose-built for the rugged, often harsh environments of operational technology (OT) in industries like manufacturing, mining, oil & gas, utilities, and transportation. They focus on secure, reliable connectivity for sensors, machines, and control systems.

- Key Features:
    - Ruggedized Hardware: Industrial-grade switches, routers, and wireless access points designed to withstand extreme temperatures, vibration, shock, dust, and moisture.
    - OT/IT Convergence: Bridging the gap between traditional IT networks and operational technology (OT) networks, allowing for centralized management and enhanced security.
    - Support for Industrial Protocols: Compatibility with common industrial protocols (e.g., EtherNet/IP, PROFINET, Modbus TCP, DNP3) to ensure

seamless communication with industrial control systems (ICS) and SCADA.
    - Edge Compute Capabilities: Built-in processing power at the edge of the network for local data analysis and faster decision-making, reducing reliance on the cloud.
    - Enhanced Cybersecurity for OT: Specialized security features to protect industrial control systems from cyber threats, including network segmentation and visibility into OT device behavior (e.g., Cisco Cyber Vision).
    - Flexible Connectivity: Support for various wired and wireless technologies including industrial Ethernet, Wi-Fi, 5G/LTE (for remote sites), and LPWAN (Low-Power Wide-Area Networks) for sensor networks.
    - Network Automation & Management: Simplified management and automation for distributed industrial networks, often leveraging familiar IT tools.

4. SD-WAN (Software-Defined Wide Area Network)

Cisco SD-WAN (primarily powered by Cisco Catalyst SD-WAN, built on Viptela technology, and also available through Meraki MX security appliances) transforms how organizations connect their branch offices, remote users, and cloud applications over the wide area network. It leverages software to intelligently route traffic, optimize application performance, and enhance security.

- Key Features:
    - Application-Aware Routing: Dynamically steers traffic over the best available link (MPLS, broadband internet, 5G/LTE) based on real-time network conditions and application performance requirements, ensuring optimal user experience for critical apps.
    - Centralized Management (vManage): A single, cloud-delivered orchestrator for configuring, monitoring, and managing the entire SD-WAN fabric, simplifying policy enforcement and troubleshooting.
    - Cost Efficiency: Enables organizations to leverage less expensive internet broadband connections without sacrificing performance or reliability, reducing reliance on costly MPLS circuits.
    - Integrated Security: Built-in security features like enterprise firewalls, IPS, URL filtering, malware protection, and IPsec VPN for secure communication across the WAN. Supports SASE (Secure Access Service Edge) integration.
    - Cloud OnRamp: Secure and optimized direct connectivity to major public cloud providers and SaaS applications, improving performance for cloud-first strategies.

    - Zero-Touch Provisioning (ZTP): Simplifies the deployment of new branch offices by allowing devices to self-provision, reducing the need for on-site IT staff.
    - Visibility and Analytics: Provides deep insights into network performance, application behavior, and security posture across the entire WAN.
    - High Availability: Automatic failover and load balancing across multiple transport links to ensure continuous network uptime.

5. Smart Buildings

Cisco's smart building solutions leverage the network as the foundational platform to converge traditionally disparate building systems (like HVAC, lighting, security, and access control) onto a single, intelligent IP infrastructure. This leads to greater efficiency, sustainability, and improved occupant experience.

- Key Features:
    - Converged IP Network: A unified, secure IP network backbone that supports all building systems, simplifying cabling, reducing infrastructure costs, and enabling centralized management.
    - Power over Ethernet (PoE/UPOE+): Provides both data connectivity and power over a single Ethernet cable to various building devices (LED lighting, sensors, cameras, access points), reducing the need for separate electrical wiring and improving energy efficiency.
    - IoT Integration: Securely connects and manages a wide array of IoT sensors and devices for real-time data collection (occupancy, temperature, air quality, light levels).
    - Building Automation System (BAS) Integration: Seamlessly integrates with building management systems, allowing for intelligent automation and control of lighting, climate, and other environmental factors.
    - Physical Security Integration: Incorporates IP video surveillance, access control systems, and other security devices onto the network.
    - Space Utilization Analytics (Cisco Spaces): Leverages Wi-Fi and IoT data to provide insights into building occupancy, flow patterns, and asset tracking, helping optimize space usage and improve employee experience.
    - Sustainability & Energy Efficiency: Enables intelligent control of building systems to reduce energy consumption and operational costs.
    - Enhanced Occupant Experience: Personalized comfort controls, seamless Wi-Fi, and integration with collaboration tools.
    - Cybersecurity for OT/Building Systems: Securing building control systems and IoT devices from cyber threats, often leveraging network segmentation and device profiling.

All Networking Solutions

This typically implies a comprehensive portfolio that includes:

- Enterprise Networking: Solutions for campus LAN, wireless LAN, branch office, and remote work connectivity, often managed by Cisco Catalyst Center (formerly DNA Center) for automation and assurance.
- Data Center Networking: As described above, focused on high-performance, automated, and secure data center fabrics.
- SD-WAN: Optimizing WAN connectivity for performance, security, and cost efficiency.
- Industrial Networking: Ruggedized solutions for operational technology environments.
- Cloud Networking: Extending network policies and security consistently to public cloud environments.
- Network Security: Security features integrated across all networking domains, including firewalls, IPS, secure access, and network segmentation.
- Network Automation & Orchestration: Tools and platforms to automate provisioning, configuration, and operations across the entire network.
- Observability & Assurance: Solutions for monitoring network health, performance, and application experience (e.g., using ThousandEyes and AppDynamics in conjunction with networking platforms).

- Security
  - AI for security
  - Data center security
  - Hybrid Mesh Firewall
  - Industrial security
  - Network security
  - Secure Access Service Edge (SASE)
  - Secure Hybrid Work
  - Zero trust
  - Collaboration
  - Customer experience
  - Event management
  - Intelligent workspaces
  - IT administration
  - Remote work

Security: Comprehensive Protection for Modern Threats

Cisco's security portfolio is designed to provide end-to-end protection across the

entire attack surface, from endpoints and networks to the cloud and applications. Their strategy emphasizes integration, automation, and threat intelligence.

1. AI for Security

This refers to the application of Artificial Intelligence and Machine Learning (AI/ML) techniques to enhance security capabilities, moving beyond traditional signature-based detection to more proactive and intelligent threat analysis.

- Key Features/Benefits:
    - Advanced Threat Detection: AI/ML algorithms analyze vast datasets (network traffic, logs, endpoint behavior) to identify anomalies, zero-day attacks, and sophisticated malware that might bypass traditional defenses.
    - Automated Response: AI can trigger automated containment or remediation actions based on detected threats, reducing response times.
    - Behavioral Analytics: Learning normal user and device behavior to detect deviations that could indicate compromise (e.g., insider threats, compromised accounts).
    - Encrypted Traffic Analytics (ETA): Analyzing patterns in encrypted network traffic to detect threats without decrypting the data, preserving privacy while maintaining visibility.
    - Threat Intelligence: AI-powered analysis of global threat data (from Cisco Talos) to provide real-time updates and predictive insights.
    - AI-specific Security: Cisco is also developing solutions like Cisco AI Defense to secure AI applications and workloads themselves, protecting against prompt injection, data leakage from LLMs, and adversarial AI attacks. This includes identifying and managing sanctioned vs. shadow AI applications.
- Cisco Examples: Cisco Secure Network Analytics (Stealthwatch), Cisco Secure Endpoint, Cisco Secure Firewall, Cisco Umbrella, and the broader Cisco Security Cloud all leverage AI/ML for enhanced detection and response.

2. Data Center Security

Securing the heart of the enterprise, data center security focuses on protecting critical applications, data, and infrastructure within on-premises data centers and hybrid cloud environments.

- Key Features/Benefits:
    - Zero Trust Architecture: Implementing granular access controls based on continuous verification of users, devices, and applications, regardless of their location (inside or outside the traditional perimeter).
    - Secure Segmentation & Microsegmentation: Dividing the network into smaller, isolated segments and microsegments (e.g., per application,

workload, or even container) to limit the lateral movement of threats within the data center, often achieved with Cisco ACI.
    - Next-Generation Firewalls (NGFWs): Deploying high-performance firewalls at the data center perimeter and internal segments for deep packet inspection, intrusion prevention, and advanced malware protection (e.g., Cisco Secure Firewall).
    - Cloud Security Integration: Extending consistent security policies and controls to public cloud environments, ensuring secure connections and data flows between on-premises and cloud resources.
    - Visibility & Analytics: Comprehensive monitoring of data center traffic and application behavior to detect threats and abnormal activity.
    - Identity Services Engine (ISE): Centralized policy management for authentication and network access control for users and devices connecting to data center resources.
- Cisco Examples: Cisco Secure Firewall, Cisco ACI, Cisco Identity Services Engine (ISE), Cisco Secure Network Analytics, Cisco Multicloud Defense.

3. Hybrid Mesh Firewall

This is a modern approach to firewall deployment that extends consistent security policies across a distributed, hybrid environment, encompassing on-premises data centers, private clouds, and multiple public clouds. It aims to provide unified firewall management and enforcement everywhere applications and data reside.

- Key Features/Benefits:
    - Consistent Policy Enforcement: Applying the same security policies regardless of where the workload or application is hosted (on-prem, private cloud, public cloud).
    - Centralized Management: A single management plane to configure, monitor, and update firewalls deployed across diverse environments, simplifying operations.
    - Automated Provisioning: Automating the deployment and scaling of firewall instances across hybrid environments to keep pace with dynamic workloads.
    - Multi-Cloud Visibility: Providing unified visibility into network traffic and security events across different cloud providers.
    - Seamless Cloud Integration: Native integration with public cloud infrastructure and services.
    - Reduced Complexity: Consolidating firewall management and reducing the operational overhead of managing disparate security tools.
- Cisco's Approach: Cisco's Hybrid Mesh Firewall strategy integrates its Secure Firewall (including virtual firewalls) with solutions like Cisco Multicloud Defense and centralized management tools to deliver this distributed, unified firewall capability.

4. Industrial Security

Focused on protecting Operational Technology (OT) and Industrial Control Systems (ICS) in critical infrastructure, manufacturing, energy, and other industrial environments. This addresses the unique challenges of securing highly specialized and often legacy systems.

- Key Features/Benefits:
    - OT Visibility & Asset Inventory: Discovering all connected industrial assets (PLCs, RTUs, sensors) and gaining deep visibility into their communications and vulnerabilities (e.g., Cisco Cyber Vision).
    - Segmentation for OT: Implementing network segmentation and microsegmentation within industrial networks (using zones and conduits) to prevent the spread of threats and enforce least-privilege access.
    - Threat Detection for ICS: Detecting cyber threats specifically targeting industrial protocols and control systems.
    - Ruggedized Security Appliances: Industrial-grade firewalls and security devices designed to operate in harsh environmental conditions (e.g., Cisco Secure Firewall ISA3000).
    - Secure Remote Access: Providing secure remote access for OT engineers and technicians to industrial equipment without compromising security.
    - IT/OT Convergence: Integrating IT security operations centers (SOCs) with OT security insights for a unified view of threats across the enterprise.
- Cisco Examples: Cisco Cyber Vision, Cisco Secure Firewall ISA3000, Cisco Identity Services Engine (ISE) for extending IT policies to OT, Cisco Secure Remote Worker.

5. Network Security

The foundational layer of security, protecting the network infrastructure itself and all traffic flowing through it.

- Key Features/Benefits:
    - Next-Generation Firewalls (NGFWs): Deep packet inspection, intrusion prevention system (IPS), advanced malware protection (AMP), application visibility and control (e.g., Cisco Secure Firewall).
    - Network Access Control (NAC): Authenticating and authorizing all devices and users attempting to connect to the network, ensuring compliance (e.g., Cisco Identity Services Engine - ISE).
    - DNS-Layer Security: Blocking access to malicious domains and IPs at the DNS layer before a connection is even established (e.g., Cisco Umbrella).
    - Intrusion Detection/Prevention Systems (IDS/IPS): Detecting and preventing known and unknown threats by analyzing network traffic for

malicious patterns.
    - Encrypted Traffic Analytics (ETA): As mentioned, detecting threats in encrypted traffic without decryption.
    - Network Segmentation: Isolating different parts of the network to contain breaches and enforce specific security policies.
    - VPN Solutions: Secure remote access for users and site-to-site connectivity for branches (e.g., Cisco Secure Client/AnyConnect).
- Cisco Examples: Cisco Secure Firewall, Cisco Umbrella, Cisco Identity Services Engine (ISE), Cisco Secure Network Analytics (Stealthwatch), Cisco Secure Client (AnyConnect).

6. Secure Access Service Edge (SASE)

SASE (pronounced "sassy") is a cloud-delivered architecture that converges networking (SD-WAN) and security functions (like SWG, CASB, ZTNA, FWaaS) into a single, integrated service model. It's designed for the modern, distributed workforce and cloud-centric applications.

- Key Features/Benefits:
    - Convergence: Unifies network connectivity and security into a single cloud-native service, simplifying management and reducing complexity.
    - Identity-Driven Access: Access policies are based on user and device identity, not just network location.
    - Cloud-Delivered Security: Security functions are delivered from the cloud edge, closer to users and cloud applications, ensuring consistent protection regardless of location.
    - Optimized Performance: Direct-to-internet access for cloud applications, improving performance by bypassing traditional centralized data center security stacks.
    - Reduced Cost & Complexity: Consolidates multiple point products into a single platform, simplifying operations and potentially reducing costs.
    - Secure Remote Work: Provides secure and seamless access for remote and hybrid workers to any application from any device.
- Cisco's Approach: Cisco's SASE solution brings together Cisco SD-WAN, Cisco Umbrella (for cloud security functions like SWG, CASB, DNS security), Cisco Secure Access (Zero Trust Network Access), and other security capabilities under a unified management plane. Cisco+ Secure Connect is their "SASE as-a-service" offering.

7. Secure Hybrid Work

This comprehensive solution set focuses on securing employees, data, and applications regardless of where work happens – in the office, at home, or on the go. It's a holistic strategy combining networking, security, and collaboration tools.

- Key Features/Benefits:
    - Zero Trust Access: Verifying every user and device before granting least-privilege access to applications and data.
    - Secure Connectivity: Providing reliable and secure VPN access (AnyConnect), as well as SASE capabilities for direct-to-cloud security.
    - Endpoint Security: Protecting laptops, mobile devices, and other endpoints from malware and advanced threats.
    - Email Security: Defending against phishing, malware, and other email-borne threats.
    - Cloud Security: Securing access to SaaS applications and protecting data in cloud environments.
    - Secure Collaboration: Ensuring that communication and content sharing through collaboration tools (e.g., Webex) are fully encrypted and protected.
    - Unified Visibility & Management: Providing IT and security teams with a unified view of security posture across all work environments.
- Cisco Examples: Cisco Secure Access (Duo for MFA/ZTNA), Cisco Umbrella, Cisco Secure Client (AnyConnect), Cisco Secure Endpoint, Cisco Secure Email, Cisco Secure Firewall, and Webex with its integrated security features.

8. Zero Trust

Zero Trust is a security philosophy and architectural model that operates on the principle of "never trust, always verify." It assumes that no user, device, or application should be inherently trusted,[1] regardless of whether it's inside or outside the traditional network perimeter.

- Key Principles & Features:
    - Verify Explicitly: All access requests are authenticated and authorized based on all available data points, including user identity, device posture, location, and application context.
    - Least Privilege Access: Users and devices are granted only the minimum access necessary to perform their tasks, reducing the attack surface.
    - Assume Breach: Security teams assume that breaches will occur and design defenses to minimize their impact and prevent lateral movement.
    - Continuous Verification: Trust is never permanent; authentication and authorization are continuously reassessed based on changes in context.
    - Microsegmentation: Granular network segmentation to isolate workloads and control communication flow.
    - Visibility & Analytics: Comprehensive logging and monitoring to detect anomalous behavior.
- Cisco's Approach: Cisco implements Zero Trust across its portfolio through:
    - Workforce Zero Trust: Using Cisco Duo for multi-factor authentication (MFA), device trust, and secure access to applications.
    - Workload Zero Trust: Implementing microsegmentation within data centers and cloud environments with Cisco ACI and Multicloud Defense.

    - Workplace Zero Trust: Leveraging Cisco Identity Services Engine (ISE) for network access control and segmentation within the office environment.

Collaboration: Connecting People and Teams

Cisco's collaboration solutions focus on enabling seamless communication and teamwork, regardless of location or device, with Webex as its flagship platform.

- Key Features/Benefits (across the categories below):
    - Unified Experience: Integrating meetings, messaging, calling, and events into a single, consistent platform.
    - AI-Powered: Using AI for noise removal, transcription, translation, intelligent summaries, and virtual assistants.
    - Immersive Video: High-definition video, intelligent framing, and virtual backgrounds.
    - Secure by Design: End-to-end encryption, robust access controls, and compliance features.
    - Device Integration: Seamless experience with a wide range of Cisco Webex devices (room systems, desk devices, cameras, headsets).
    - Scalability: Supporting everything from 1:1 chats to large-scale virtual events.

1. Customer Experience

This refers to how Cisco's collaboration tools, particularly Webex, are used to enhance interactions with external customers, often in contact center environments.

- Key Features:
    - Webex Contact Center: Cloud-based contact center solution with intelligent routing, omnichannel support (voice, chat, email, social), and integration with CRM systems.
    - Webex Contact Center AI Solutions: AI-powered virtual agents (chatbots, voicebots) for self-service, agent assist tools (suggested responses, sentiment analysis), and post-call analytics.
    - Webex Workforce Optimization (WFO): Tools for agent scheduling, performance monitoring, quality management, and training.
    - CPaaS (Communications Platform as a Service) with Webex Connect: Allows businesses to integrate communication capabilities directly into their applications and workflows for personalized customer journeys (e.g., automated notifications, two-way SMS).
    - Personalized Engagement: Tailoring customer interactions based on context and preferences.

2. Event Management

Solutions for planning, hosting, and managing virtual, hybrid, and in-person events of various scales.

- Key Features:
    - Webex Events (formerly Socio): End-to-end event management platform for registration, ticketing, mobile event apps, attendee engagement, live streaming, and post-event analytics.
    - Hybrid Event Support: Capabilities to seamlessly blend in-person and virtual audiences, ensuring a consistent experience for all participants.
    - Production Studio: Tools for creating professional, branded live streams.
    - Engagement Features: Interactive Q&A, polls, breakout rooms, networking lounges, and gamification.
    - Scalability: Supports events from small webinars to large conferences with tens of thousands of attendees.

3. Intelligent Workspaces

Focuses on transforming physical office spaces and home offices into smart, collaborative, and productive environments using integrated technology.

- Key Features:
    - Webex Devices: Smart room systems (Webex Room Series), personal desk devices (Webex Desk Series), and interactive whiteboards (Webex Board) with integrated cameras, microphones, and speakers.
    - AI-Powered Meeting Rooms: Intelligent camera framing (auto-framing, speaker tracking, people focus), noise removal, and AI assistants to enhance the meeting experience.
    - Environmental Sensors (Meraki MT): Monitoring temperature, humidity, air quality, and occupancy in meeting rooms and common areas.
    - Space Utilization Analytics (Cisco Spaces): Providing insights into how office spaces are being used to optimize layouts and resource allocation.
    - Seamless User Experience: Proximity join, wireless content sharing, and integration with calendar systems for easy meeting starts.
    - PoE-Powered Lighting & HVAC Control: Converging building systems onto the network for centralized, intelligent control.
- Cisco Examples: Webex Devices, Cisco Meraki MT sensors, Cisco Spaces, Cisco IP phones, Cisco Catalyst switches with UPOE.

4. IT Administration

Tools and platforms that simplify the management, monitoring, and troubleshooting of Cisco's diverse technology portfolio, empowering IT teams.

- Key Features:

    - Cisco Control Hub: A unified, cloud-based management portal for Webex collaboration services, allowing IT admins to provision users, manage devices, configure policies, and monitor usage and quality.
    - Cisco Catalyst Center (formerly DNA Center): A centralized network controller and management platform for automating network provisioning, policy enforcement, and providing assurance and analytics for enterprise wired and wireless networks.
    - Cisco Intersight: A cloud-based management platform for Cisco UCS and HyperFlex, providing intelligent automation, orchestration, and lifecycle management for data center infrastructure.
    - Cisco Meraki Dashboard: The single pane of glass for managing all Meraki cloud-managed devices (wireless, switches, security, cameras).
    - Cisco SecureX: A cloud-native platform that unifies visibility, enables automation, and strengthens security operations across Cisco's security portfolio and integrated third-party tools.
    - ThousandEyes: Provides deep visibility into network and application performance across the internet and cloud, aiding in troubleshooting.
    - APIs & Automation: Extensive APIs across platforms enable IT to automate tasks and integrate with existing IT Service Management (ITSM) systems.

5. Remote Work

Solutions specifically designed to enable employees to work securely and productively from any location outside the traditional office. This often overlaps heavily with Secure Hybrid Work.

- Key Features:
    - Secure Connectivity: VPN solutions (Cisco Secure Client/AnyConnect), Secure Access Service Edge (SASE) for secure, direct-to-cloud access.
    - Collaboration Tools: Full suite of Webex applications (meetings, messaging, calling) for seamless communication and teamwork from home.
    - Endpoint Security: Protecting remote laptops, desktops, and mobile devices from malware and threats (Cisco Secure Endpoint).
    - Multi-Factor Authentication (MFA): Strong identity verification for remote access (Cisco Duo).
    - Cloud-Delivered Security: Protecting users Browse the internet and accessing SaaS applications from home (Cisco Umbrella).
    - Home Office Devices: Cisco Webex Desk devices and headsets designed for optimal remote work experience.
    - IT Visibility & Management: Tools to monitor and troubleshoot remote worker experiences and device health.

- Cisco's Approach: Cisco provides a comprehensive remote work solution that integrates security, collaboration, and networking capabilities to ensure a secure, productive, and consistent experience for employees working from anywhere. This is largely encompassed by their broader "Secure Hybrid Work" strategy.

- Computing
  - Converged infrastructure
  - Hybrid cloud
  - Hyperconverged
  - Virtual desktop infrastructure

Computing: Data Center and Cloud Infrastructure

1. Converged Infrastructure (CI)

Converged Infrastructure is a hardware-centric approach to data center management where multiple IT components (compute, storage, and networking) are pre-packaged, pre-configured, and pre-tested by a single vendor. It essentially consolidates these discrete components into a unified system that is easier to deploy and manage.

- Key Characteristics:
  - Bundled Components: Servers (compute), storage arrays (SAN/NAS), network switches, and often virtualization software are sold as a single SKU.
  - Single Vendor Integration: The components are typically from a single vendor or a tightly integrated partnership, ensuring compatibility and simplified support.
  - Hardware-Defined: While it includes software, the core convergence is at the hardware layer.
  - Centralized Management (often): Aims to provide a simpler management interface, though it may still involve separate tools for each component within the bundle.
  - Faster Deployment: Because it's pre-integrated, deployment time is significantly reduced compared to assembling disparate components.
  - Examples: Cisco's partnership with NetApp for FlexPod (Cisco UCS + Cisco Nexus + NetApp Storage) is a prime example of a leading Converged Infrastructure solution. Other vendors like HPE (ConvergedSystem) also offer CI.
- Benefits: Reduces complexity, speeds up deployment, simplifies procurement, and provides a single point of contact for support.
- Cisco's Role: Cisco provides the unified compute (UCS) and networking (Nexus)

elements that are foundational to many CI solutions, often partnering with storage vendors.

2. Hybrid Cloud

Hybrid cloud refers to an IT environment that combines elements of both public cloud (e.g., AWS, Azure, Google Cloud) and private cloud (on-premises data centers or dedicated private cloud infrastructure), allowing data and applications to be shared and orchestrated across these different environments.

- Key Characteristics:
    - Interconnected Environments: Public cloud resources are seamlessly integrated with private cloud/on-premises infrastructure.
    - Workload Portability: The ability to move applications and data between public and private clouds to optimize for cost, performance, security, or compliance.
    - Unified Management (Desired): The goal is to manage both environments from a single console, though achieving this comprehensively can be complex.
    - Orchestration and Automation: Tools are crucial for automating the deployment, scaling, and management of workloads across environments.
    - Flexibility: Organizations can choose the best environment for each workload based on specific requirements (e.g., sensitive data stays on-prem, burstable workloads go to public cloud).
- Benefits: Provides the scalability and flexibility of public cloud with the control and security of private cloud, enabling greater agility and cost optimization.
- Cisco's Role: Cisco provides critical components for hybrid cloud, including:
    - Cloud Interconnect: Secure and optimized networking for connecting on-premises data centers to public clouds.
    - Cloud Security: Extending consistent security policies across hybrid environments (e.g., Cisco Multicloud Defense, Secure Firewall).
    - Cloud Management & Orchestration: Tools like Cisco Intersight and AppDynamics for visibility, automation, and performance monitoring across hybrid cloud infrastructure and applications.
    - Container Platforms: Solutions for deploying and managing containerized applications that can run consistently across hybrid environments.

3. Hyperconverged (HCI)

Hyperconverged Infrastructure (HCI) is a software-defined, scale-out architecture that tightly integrates compute, storage, and networking into a single, highly virtualized software-defined solution running on industry-standard x86 servers (nodes). Unlike

traditional CI, HCI collapses the entire stack into a single "building block."

- Key Characteristics:
    - Software-Defined: All core functions (compute, storage, networking) are abstracted and managed through software, typically at the hypervisor level.
    - Distributed Architecture: Resources are pooled across a cluster of nodes, making it easy to scale by simply adding more nodes.
    - Commodity Hardware: Runs on standard x86 servers with local storage, reducing reliance on expensive, specialized hardware.
    - Unified Management: Managed from a single, often hypervisor-integrated, interface.
    - Scale-Out: Designed for incremental growth by adding nodes to the cluster.
    - Eliminates SAN/NAS: Local storage within each node is pooled and managed by the HCI software layer, removing the need for a separate storage area network (SAN) or network-attached storage (NAS).
- Benefits: Simplified management, rapid deployment, lower total cost of ownership (TCO), easier scalability, and increased agility. It's particularly popular for virtual desktop infrastructure (VDI), remote office/branch office (ROBO), and consolidating mixed workloads.
- Cisco's Role: Cisco's primary HCI offering is Cisco HyperFlex, which integrates Cisco UCS servers with a distributed software layer for compute, storage, and networking.

4. Virtual Desktop Infrastructure (VDI)

Virtual Desktop Infrastructure (VDI) is a technology that hosts desktop environments (operating systems, applications, and data) on a centralized server within a data center or cloud, and delivers them to end-user devices (PCs, thin clients, tablets, smartphones) over a network. Users access their personalized virtual desktops remotely.

- Key Characteristics:
    - Centralized Management: Desktops are managed centrally, simplifying patching, updates, and application deployment.
    - Any Device, Anywhere Access: Users can access their corporate desktop environment from various devices and locations with an internet connection.
    - Enhanced Security: Data resides in the data center, not on the endpoint, reducing the risk of data loss if a device is stolen or compromised. Policies and security updates are applied centrally.
    - Data Protection: Centralized storage simplifies backup and disaster recovery.
    - Cost Efficiency (potentially): Can reduce endpoint hardware costs (using

thin clients) and simplify IT management.
    - User Experience: Can offer a consistent and personalized desktop experience, whether persistent (changes saved) or non-persistent (resets after each session).
- Benefits: Improved data security, simplified desktop management, increased user mobility, and enhanced business continuity.
- Cisco's Role: While VDI solutions are often built on platforms like VMware Horizon or Citrix DaaS, Cisco provides the foundational infrastructure elements that make VDI possible and performant:
    - Compute: Cisco UCS servers provide the high-density, high-performance compute needed to host a large number of virtual desktops.
    - Networking: Cisco Nexus switches and Catalyst switches provide the low-latency, high-bandwidth network connectivity essential for a smooth VDI experience.
    - Hyperconverged Infrastructure (HCI): Cisco HyperFlex is a very popular platform for VDI deployments due to its simplified management, predictable performance, and scalability.
    - Security: Solutions like Cisco Secure Access (Duo) and network segmentation (ISE) ensure secure access to VDI environments.

Services Section

Customer Experience (CX) Services

- Lifecycle Services
- Solution support
- Hardware support
- Software support
- Packaged services
- Solution consulting
- Cisco learning
- Customer stories

Customer Experience (CX) Services

This is the overarching philosophy and portfolio of services designed to help customers achieve business outcomes, reduce risk, and minimize effort throughout their technology journey. CX aims to proactively guide customers from planning and implementation to ongoing optimization and adoption, ensuring they extract maximum value from their Cisco investments. It encompasses a range of offerings, from foundational support to strategic consulting.

1. Lifecycle Services

Cisco's Lifecycle Services are built around a structured methodology, typically the PPDIOO (Prepare, Plan, Design, Implement, Operate, Optimize) model, which outlines the phases of a successful technology deployment and ongoing management. These services ensure that technology is adopted effectively and delivers sustained value.

- Prepare: High-level analysis of business requirements, technical strategies, and existing infrastructure to identify appropriate solutions.
- Plan: Detailed assessment of current network, staff, and processes; development of a comprehensive project plan, including resource allocation, timelines, and risk mitigation.
- Design: Creation of detailed network and system designs that meet business and technical requirements, addressing scalability, availability, security, and performance.
- Implement: Deployment and configuration of hardware and software, integration with existing systems, and migration of data/applications.
- Operate: Ongoing monitoring, management, and troubleshooting of the network and solutions, including proactive maintenance and incident management.
- Optimize: Continuous improvement of network performance, security posture, and efficiency; capacity planning, technology adoption driving, and maximizing ROI.

2. Solution Support

Cisco Solution Support is a specialized level of technical support designed for complex, multi-product, and often multi-vendor IT environments. Its key differentiator is providing a single, centralized point of contact and accountability for resolving issues that may span across Cisco products and eligible third-party solutions.

- Centralized Point of Contact: Customers deal with a single, designated solution expert who manages the entire case from initiation to resolution.
- Multi-Vendor Coordination: Cisco takes on the responsibility of coordinating with other solution vendors on the customer's behalf, streamlining troubleshooting for integrated solutions.
- Accelerated Resolution: Designed to speed up problem diagnosis and resolution in complex environments, minimizing downtime.
- Solution-Level Expertise: Access to highly skilled engineers with deep knowledge of how various Cisco and partner technologies interact within a solution.

3. Hardware Support (e.g., Cisco Smart Net Total Care - SNTC)

This category focuses on providing technical support and replacement services for Cisco hardware products. It ensures the physical infrastructure remains operational and helps minimize downtime from hardware failures.

- Technical Assistance Center (TAC) Access: 24/7 access to Cisco's global team of expert engineers for troubleshooting hardware issues.
- Hardware Replacement: Fast and reliable replacement of faulty hardware, with various service level options (e.g., Next Business Day (NBD), 4-hour, or 2-hour delivery) depending on criticality.
- Onsite Field Engineer Option: For critical issues, the ability to dispatch a field engineer to the customer's site for hardware replacement or repair.
- Device Diagnostics and Alerts: Proactive monitoring tools that detect potential hardware issues and generate alerts.
- Online Resources: Access to Cisco.com's extensive knowledge base, documentation, and tools.
- Product Lifecycle Management: Provides insights into end-of-life (EOL) and end-of-sale (EOS) dates to aid in refresh planning.

4. Software Support (Cisco Software Support Service - SWSS)

Cisco Software Support Service (SWSS) ensures that Cisco software applications and licensed features are always current, performing optimally, and supported effectively.

- Software Updates & Upgrades: Access to major, minor, and maintenance releases, including new features, enhancements, security patches, and bug fixes, ensuring software stays up-to-date and secure.
- Technical Assistance Center (TAC) Access: 24/7 access to Cisco TAC experts for software-related troubleshooting and guidance.
- Online Support Resources: Access to Cisco's online knowledge base, forums, and interactive troubleshooting tools.
- License Management Support: Assistance with managing software licenses and ensuring compliance.
- Proactive Alerts: Notifications about software vulnerabilities, product advisories, and critical updates.

5. Packaged Services

Cisco Packaged Services are pre-defined, standardized, and often fixed-price service offerings designed for rapid deployment, simplified ordering, and predictable outcomes for common technology implementations or operational tasks. They offer a structured approach to address specific customer needs efficiently.

- Standardized Scope: Clear, defined deliverables and activities for specific tasks (e.g., quick-start deployments, basic configurations, health checks for particular products).
- Accelerated Deployment: Designed for quick implementation, leveraging best practices and often automation.
- Predictable Pricing & Outcomes: Transparent pricing and clear expectations for the results of the service.

- Reduced Complexity: Simplifies the process of acquiring and deploying services, especially for common scenarios or organizations with limited custom needs.
- Examples: Could include a "Meraki Wireless Quick Start," a "Webex Rooms Deployment Service," or a "Secure Endpoint Installation Service."

6. Solution Consulting

Cisco Solution Consulting provides strategic and expert guidance to help organizations leverage Cisco technologies to achieve specific business outcomes and navigate complex IT challenges. It offers prescriptive advice and tailored roadmaps.

- Strategic Advisory: Assisting organizations in aligning IT strategy with business goals, including digital transformation initiatives.
- Technology & Architecture Design: Providing expert advice on technology selection, designing customized solution architectures, and integrating various Cisco products with existing infrastructure.
- Assessment Services: Conducting in-depth assessments of current environments (network, security, cloud readiness, collaboration posture) to identify gaps, risks, and opportunities.
- Optimization Recommendations: Providing guidance on optimizing existing Cisco deployments for performance, security, and efficiency.
- Roadmap Development: Helping organizations create phased plans for technology adoption and modernization.

7. Cisco Learning

Cisco Learning offers a wide array of training and certification programs designed to educate IT professionals, developers, and network engineers on Cisco technologies. It aims to build and validate the skills needed to design, implement, operate, and optimize Cisco solutions.

- Certification Programs: Industry-recognized certifications (e.g., CCNA, CCNP, CCIE, DevNet) that validate expertise in various Cisco technologies.
- Training Courses: A comprehensive catalog of courses (instructor-led, online, self-paced, virtual labs) covering a broad range of Cisco products and technologies.
- Cisco U. (Digital Learning Platform): A personalized digital learning experience offering access to in-depth training, labs, and certification preparation.
- DevNet Learning: Resources specifically for developers, focusing on programmability, automation, and API integration.
- Hands-on Labs: Provides access to virtual lab environments for practical experience.

8. Customer Stories

Cisco leverages customer stories (case studies, testimonials, videos, webinars) to

showcase how organizations have successfully implemented Cisco services and technologies to achieve tangible business outcomes.

- Real-World Validation: Provides concrete examples of how businesses have overcome challenges and achieved success using Cisco's products and services.
- Outcome-Focused: Highlights specific improvements in areas like operational efficiency, cost reduction, enhanced security, improved customer experience, and accelerated digital transformation.
- Credibility & Trust: Builds trust by demonstrating proven results and showcasing satisfied customers.
- Inspiration & Best Practices: Offers insights and inspiration for prospective customers facing similar challenges, often categorized by industry or solution area.

Professional Services

- Security assessment and consulting
- Implementation and deployment services
- Custom solution development
- Security architecture design

Professional Services

1. Security Assessment and Consulting

This service involves expert analysis of an organization's current security posture, identifying vulnerabilities, risks, and compliance gaps, and then providing strategic recommendations to improve overall cybersecurity. It's a foundational step for many organizations looking to strengthen their defenses.

- Key Features/Activities:
    - Vulnerability Assessments: Identifying weaknesses in networks, systems, and applications that attackers could exploit.
    - Penetration Testing (Pen Testing): Simulating real-world cyberattacks to uncover exploitable vulnerabilities and evaluate the effectiveness of existing security controls.
    - Risk Assessments: Identifying, analyzing, and evaluating information security risks to determine their potential impact on business operations.
    - Compliance Audits & Readiness: Assessing an organization's adherence to regulatory requirements (e.g., GDPR, HIPAA, PCI DSS, NIST) and providing guidance for achieving compliance.
    - Security Posture Review: A holistic evaluation of an organization's

security programs, policies, procedures, and technologies.
    - Threat Modeling: Identifying potential threats and vulnerabilities from an attacker's perspective.
    - Incident Response Preparedness: Assessing an organization's ability to detect, respond to, and recover from security incidents.
    - Security Strategy Development: Advising on the creation of a comprehensive, multi-year security roadmap aligned with business objectives.
- Benefits: Proactive risk reduction, compliance assurance, improved security posture, data protection, and a clear roadmap for security investments.
- Cisco's Role: Leveraging its deep expertise in cybersecurity and threat intelligence (Cisco Talos), Cisco's consultants help customers understand their unique threat landscape and build resilient security programs.

2. Implementation and Deployment Services

These services focus on the practical execution of installing, configuring, and integrating new Cisco technologies and solutions within a customer's existing IT environment. They ensure that solutions are deployed correctly, efficiently, and according to best practices.

- Key Features/Activities:
    - Solution Installation: Physical installation of hardware (servers, switches, routers, firewalls, access points, devices).
    - Configuration: Configuring software, operating systems, applications, and network devices according to design specifications.
    - Integration: Ensuring seamless interoperability between new Cisco solutions and existing IT infrastructure, applications, and third-party systems.
    - Migration: Assisting with the transfer of data, applications, and services from old systems to new ones with minimal disruption.
    - Testing & Validation: Thoroughly testing the deployed solution to ensure it meets performance, functionality, and security requirements.
    - Knowledge Transfer: Training the customer's internal IT staff on how to operate and manage the new solution.
    - Project Management: Providing structured project management to ensure deployments are on time and within budget.
- Benefits: Faster time to value, reduced deployment risks, adherence to best practices, optimized performance from day one, and minimized disruption to business operations.
- Cisco's Role: Cisco's professional services teams, or certified partners, bring deep product knowledge and deployment experience, ensuring complex solutions like ACI, SD-WAN, or large-scale collaboration rollouts are successful.

3. Custom Solution Development

This service goes beyond standard product deployments to create tailored software, integrations, or specific functionalities that address unique customer requirements not met by off-the-shelf solutions. This often involves leveraging Cisco's platforms and APIs.

- Key Features/Activities:
    - Requirements Gathering: Detailed understanding of the customer's specific business processes and unique challenges that require a custom approach.
    - Software/Script Development: Creating custom code, scripts, or applications to extend the functionality of Cisco products or integrate them with proprietary systems.
    - API Integration: Developing custom integrations between Cisco platforms (e.g., DNA Center, Intersight, Webex, SecureX) and third-party applications or IT systems using their APIs.
    - Automation Playbook Development: Crafting bespoke automation workflows and playbooks tailored to a customer's operational procedures.
    - Proof of Concept (PoC) & Prototyping: Building small-scale models to validate custom solutions before full development.
    - System Customization: Modifying or extending existing Cisco platforms to fit specific operational or reporting needs.
- Benefits: Solutions precisely tailored to unique business needs, competitive differentiation, enhanced efficiency for specific workflows, and maximizing the value of existing technology investments through deeper integration.
- Cisco's Role: Cisco leverages its DevNet community, specialized engineers, and deep knowledge of its product APIs to build custom solutions that extend the value of its core platforms.

4. Security Architecture Design

This service involves designing a holistic, strategic security framework for an organization, outlining how various security technologies, policies, and processes will work together to achieve desired security outcomes. It's a high-level, strategic planning service.

- Key Features/Activities:
    - Current State Analysis: Evaluating existing security architecture, identifying weaknesses, redundancies, and gaps.
    - Future State Definition: Designing a target security architecture that aligns with the organization's business objectives, risk tolerance, and compliance requirements.
    - Security Control Mapping: Determining which security controls (e.g.,

firewalls, IDS/IPS, NAC, SIEM, ZTNA, SASE) are needed and where they should be placed within the infrastructure.
    - Policy & Governance Development: Advising on the creation of security policies, standards, and governance frameworks.
    - Technology Selection & Integration Strategy: Recommending specific security products (Cisco and potentially others) and outlining how they will integrate to form a cohesive defense.
    - Reference Architectures: Providing architectural blueprints and best practices for various security domains (e.g., data center security, cloud security, remote work security).
    - Roadmap Creation: Developing a phased plan for implementing the new security architecture over time.
    - Threat Landscape Context: Incorporating understanding of the organization's specific threat landscape and industry-specific risks into the design.
- Benefits: A robust and resilient security posture, effective risk management, optimized security investments, streamlined operations, and clear path to future security enhancements.
- Cisco's Role: Cisco's security architects bring deep expertise in network security, cloud security, endpoint security, and threat intelligence to design comprehensive, integrated, and future-proof security architectures for enterprises of all sizes.

Take Action [182]

- Portal Login [183]
- Managed Services Program [184]
- Become a Partner [185]
- Request Access [186]
- Find a Partner [187]
- Investor Relations [192]

Additional Resources [201]

- Resources [202]
- Documentation and Resources [203]
- Training and Certification [204]
- Developer Resources [205]

- Community and Support [206]
- Events and Webinars [207]

Key Resource Highlights [213]

- Cisco Live: Global technology conference and learning event [214]
- Cisco U. Spotlight: Learn. Connect. Innovate. [215]
- Training: Professional development and certification programs [216]
- Community: Technical forums and peer collaboration [217]

Detailed Product Information [218]

Cisco Duo - Multi-Factor Authentication & Identity Security [219]

- Overview: Cisco Duo is a comprehensive identity security platform that provides multi-factor authentication, single sign-on, and identity intelligence capabilities[220].
- Key Value Proposition: "Identity is in crisis. Duo is the cure." [221] - Duo flips the script on identity with security-first IAM that attackers hate and users love. "No phishing. No friction. No gaps." [222]
- Market Challenge Addressed: Identity is behind 60% of breaches[223]. Organizations need phishing-resistant authentication that doesn't add complexity or friction for users[224].
- Key Statistics: [225]
  - 1B+ Monthly User Authentications [226]
  - 100K+ Customers Globally [227]
  - 159% Return on Investment (ROI) [228]
  - Study by Forrester Consulting, February 2023 [229]
- Core Capabilities: [230]
  1. Phishing-resistant MFA [231]
  2. Passwordless authentication [232]
  3. Identity intelligence [233]
  4. End-to-end protection (login to enrollment, fallback, helpdesk access) [234]
  5. No extra hardware required [235]
  6. No added complexity [236]
- Customer Success Stories: [237]
  - Room & Board: 4-week rollout from start to finish [238]
  - Lyft: "One of those rare solutions that both improves the security of our company while simultaneously being easier for our employees to use" [239]

    - AmeriGas: Enables self-service, reduces help desk calls [240]
- Target Use Cases: [241]
    - Organizations addressing identity-based security challenges [242]
    - Companies seeking user-friendly security solutions [243]
    - Enterprises requiring rapid deployment [244]
    - Businesses needing self-service capabilities [245]

Cisco Hypershield - AI-Native Security Architecture [246]

- Overview: Cisco Hypershield is a groundbreaking AI-native security architecture that brings hyperscaler technology to enterprise environments, designed specifically for modern, AI-scale data centers[247].
- Key Value Proposition: "AI-native. Ever aware. Everywhere." - Bringing the power of hyperscaler technology to the enterprise[248]. Groundbreaking security architecture designed to defend modern, AI-scale data centers[249].
- Market Challenge Addressed: Traditional security approaches cannot keep pace with the scale, speed, and complexity of modern AI-driven data centers[250]. Organizations need security that adapts and scales automatically[251].
- Architectural Features: [252]
    1. AI-Native Design [253]
        - Built with AI from the ground-up [254]
        - Delivers high efficacy, faster response, and continuous protection [255]
        - Autonomous security operations with human oversight [256]
    2. Universal Protection [257]
        - End-to-end security from network to workloads [258]
        - Unified management with intelligent policy placement [259]
        - Coverage across previously inaccessible enforcement points [260]
    3. Adaptive Fabric [261]
        - Seamlessly incorporates new enforcement points [262]
        - No policy overhaul required for expansion [263]
        - Scalable and future-ready architecture [264]
- Key Capabilities: [265]
    1. Close the Exploit Gap [266]
        - Minutes versus months response time [267]
        - AI-native rule engine for vulnerability prioritization [268]
        - Surgical compensating controls deployment [269]
        - Live production traffic testing [270]
    2. Segmentation that Works [271]
        - Self-adapting network segmentation [272]
        - Real-time adaptation to current realities [273]

        - Behavior-based policy learning [274]
        - Macro-guardrails that progressively tighten [275]
    3. Self-Qualifying Updates [276]
        - Production-safe policy validation [277]
        - Dual dataplane approach for risk-free testing [278]
        - Live traffic validation before implementation [279]
- Target Use Cases: [280]
    - Modern, AI-scale data centers [281]
    - Enterprise environments requiring hyperscaler-level security [282]
    - Organizations needing adaptive, self-managing security [283]
    - Complex, dynamic network topologies [284]

Cisco Secure Endpoint - Endpoint Detection & Response [285]

- Overview: Cisco Secure Endpoint (formerly AMP for Endpoints) is a cloud-native endpoint security solution that provides comprehensive endpoint detection and response capabilities[286].
- Key Value Proposition: "Endpoint security built for resilience" - Speed matters when it comes to endpoint security[287]. Detect, respond, and recover from attacks with our cloud-native solution[288].
- Performance Metrics: [289]
    - 85% reduction in remediation times [290]
    - Cloud-native performance and scalability [291]
    - Fastest threat detection and response capabilities [292]
- Core Capabilities: [293]
    1. Powerful EDR Capabilities [294]
        - Built-in or completely managed endpoint detection and response [295]
        - Advanced threat hunting capabilities [296]
        - Integrated risk-based vulnerability management from Kenna Security [297]
    2. USB Device Control [298]
        - Granular control over approved USB devices [299]
        - Deep visibility into device events and trajectories [300]
        - Investigation capabilities for security incidents [301]
    3. Integrated XDR Capabilities [302]
        - Unified view across all security vectors [303]
        - Simplified incident management [304]
        - Automated playbooks with Cisco XDR [305]
        - Industry's broadest XDR approach [306]
    4. Built-in Talos Threat Hunting [307]
        - Proactive, human-driven threat hunting [308]

        - MITRE ATT&CK framework mapping [309]
        - Future-focused threat preparation [310]
- Integration Ecosystem: [311]
    - Cisco XDR: Unified threat detection across all vectors [312]
    - Cisco Umbrella: Always-on security for mobile users [313]
    - Cisco Duo: Identity verification before application access [314]
- Target Use Cases: [315]
    - Organizations requiring rapid threat response [316]
    - Businesses needing comprehensive endpoint visibility [317]
    - Companies seeking integrated security platforms [318]
    - Environments requiring proactive threat hunting [319]
    - Organizations with mobile and remote workforces [320]

Webex Suite - Comprehensive Collaboration Platform [321]

- Overview: Webex Suite is the world's first unified, purpose-built suite for hybrid work, providing everything businesses need to collaborate effectively[322].
- Key Value Proposition: "Everything your business needs to collaborate—in the world's first unified, purpose-built suite for hybrid work" [323]
- Core Components: [324]
    - Calling - Voice communication solutions [325]
    - Contact Center - Customer service and support solutions [326]
    - Meetings - Video conferencing and meeting solutions [327]
    - Phones, headsets, and collaboration devices - Hardware for collaboration [328]
    - Services for collaboration - Professional and support services [329]
- Target Use Cases: [330]
    - Hybrid work environments [331]
    - Enterprise collaboration [332]
    - Customer engagement [333]
    - Remote team coordination [334]
    - Unified communications [335]

Company Information - Cisco Systems [336]

Mission & Vision [337]

- Mission: To power an inclusive future for all [338]
- Vision: To be the bridge to possible [339]

Company Statistics [340]

- Employees: 80,000+ employees globally [341]
- Customers: Serving customers in 190+ countries [342]
- Market Position: Global leader in networking and cybersecurity [343]
- Innovation: Significant R&D investment in AI and security technologies [344]

Market Leadership & Customer Base [345]

- Global technology infrastructure leader [346]
- Extensive partner ecosystem [347]
- Strong presence across all major industries [348]
- Trusted by governments and enterprises worldwide [349]

What They Do [350]

- Networking infrastructure and solutions [351]
- Cybersecurity platforms and services [352]
- Collaboration and communication tools [353]
- Cloud and data center technologies [354]
- AI-powered automation and intelligence [355]

Market Trends They Address [356]

- Digital Transformation [357]
- Organizations adopting AI at unprecedented scale [358]
- Cloud-first infrastructure strategies [359]
- Hybrid work model adoption [360]
- Industrial IoT and smart building technologies [361]

AI Adoption Statistics [362]

- Mass-scale AI infrastructure deployment [363]
- AI-enabled network operations [364]
- Automated security operations [365]
- Intelligent workspaces and collaboration [366]

Network Evolution [367]

- Software-defined networking (SD-WAN) [368]
- Cloud-managed networking [369]
- Edge computing requirements [370]
- 5G and advanced connectivity [371]

Corporate Culture [372]

- Inclusive future for all [373]
- Innovation-driven organization [374]
- Customer success focus [375]
- Sustainable business practices [376]

Business Value [377]

- Simplified IT operations [378]
- Reduced operational complexity [379]
- Improved security posture [380]
- Enhanced collaboration capabilities [381]
- Accelerated digital transformation [382]

Executive Summary [383]

Cisco Systems is a global technology leader providing comprehensive networking, security, and collaboration solutions to organizations worldwide[384]. With 80,000+ employees serving customers in 190+ countries, Cisco positions itself as "the bridge to possible" in powering an inclusive future for all[385].

Key Competitive Advantages [386]

- AI-Native Approach: Leading innovation with AI-powered platforms like Hypershield and AI-enabled network operations [387]
- Platform Integration: Comprehensive solutions that eliminate complexity and provide unified management [388]
- Market Leadership: Dominant position in networking infrastructure with expanding cybersecurity portfolio [389]
- Innovation Focus: Continuous investment in emerging technologies including AI, cloud, and automation [390]
- Global Scale: Massive ecosystem of partners and customers across all industries [391]

Strategic Market Position [392]

Cisco addresses the fundamental infrastructure needs of digital transformation: [393]

- AI-scale data center requirements [394]
- Hybrid work collaboration needs [395]
- Zero trust security architecture [396]
- Cloud-native application deployment [397]
- Industrial IoT and smart building automation [398]

Investment in Innovation [399]

The company is heavily investing in: [400]

- AI-native security architecture [401]
- Mass-scale AI infrastructure [402]
- Cloud-managed networking solutions [403]
- Comprehensive threat intelligence (Talos) [404]
- Unified collaboration platforms [405]

Recommendations for Cybersecurity Company Development [406]

Based on this comprehensive analysis of Cisco Systems, here are key insights for building a cybersecurity company: [407]

Focus Areas to Consider [408]

- AI Integration: Essential for modern security and networking solutions [409]
- Platform Approach: Unified solutions vs. point products [410]
- Cloud-Native Architecture: Critical for scalability and performance [411]
- Automation: Reduce complexity and improve operational efficiency [412]

Market Opportunities [413]

- Specialized industry solutions (manufacturing, healthcare, etc.) [414]
- Small and medium business focused offerings [415]
- AI security for emerging technologies [416]

- Edge computing security solutions [417]

Key Success Factors [418]

- Strong integration capabilities across networking and security [419]
- Platform-based approach with unified management [420]
- Comprehensive partner ecosystem [421]
- Continuous innovation and R&D investment [422]
- Customer success and professional services [423]

Competitive Differentiation [424]

- Specialized vertical market focus [425]
- Innovative AI applications in security [426]
- Superior user experience and simplicity [427]
- Cost-effective solutions for specific market segments [428]
- Faster deployment and time-to-value [429]

Technology Trends to Watch [430]

- AI-native security architectures [431]
- Zero trust networking principles [432]
- Cloud-native security platforms [433]
- Automated threat response and remediation [434]
- Integrated collaboration and security solutions [435]

This comprehensive analysis provides detailed insights into Cisco's market position, technology portfolio, and strategic direction, offering valuable intelligence for cybersecurity company development and competitive positioning[436].