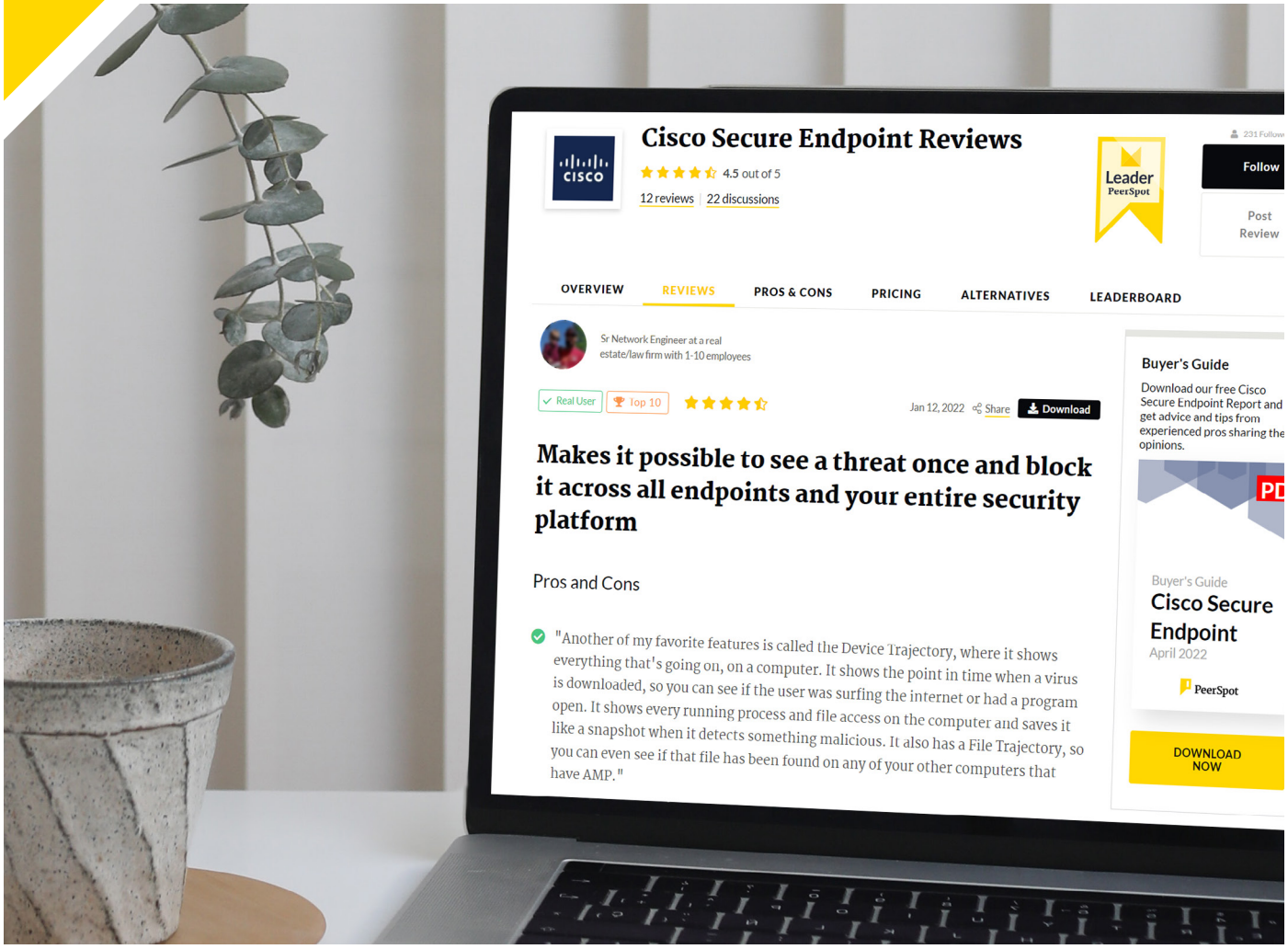
PeerPaper™ Report 2022

Based on real user reviews of Cisco Hybrid Work Solutions

Making Hybrid Work, Work Better



PeerSpot

CSO

Contents

Introduction

Hybrid work seems easy to understand. Some people work on site. Others are at home or in other remote, informal locations. Getting to success with hybrid work, in technology terms, is not so simple. IT and security teams need to provide solutions that accommodate the entire workforce, whether they are at home, in the office, or in other locations. This means staying on top of security first and foremost, with an agile, manageable toolset. No single product will deliver on hybrid work's demanding set of requirements. Cisco hybrid work solutions, bringing together a range of collaboration, security and network products, offer a cohesive solution for an organization where the need to connect everyone and everything continues to evolve with the future of work. In this paper, PeerSpot members discuss how Cisco enables the realization of such a hybrid work strategy.

Except where noted, the companies mentioned in this paper have fewer than 200 employees, though many of them work with much larger clients.

Understanding Hybrid Work

Hybrid work designs the work experience around and for the worker, wherever they are. It empowers people to work onsite, offsite, and moving between locations. The hybrid work approach also promotes inclusiveness, engagement, and well-being for all employees. Employees may be home-based. They can work from fixed offices or "nomadic" workspaces across multiple corporate sites. They can work from hotels or cafes, even airplanes. Employees might work a few days on a corporate campus, and the rest of the week on the road or at home.

The concept of hybrid work has been the subject of some industry hype, so it can be difficult to understand what's real and what matters in this emerging paradigm. A key aspect of hybrid work to grasp, however, is that it is not a temporary issue. The pandemic has created a hurried move to remote work, but hybrid work is here to stay. It's not a quick fix. Rather, it's a permanent business strategy that will continue to evolve. Solutions to address this reality must be excellent in the present, but also able to adapt as hybrid work use cases evolve over time.

One-click calling

An Overview of Cisco Hybrid Work Solutions

The Cisco hybrid work solutions brings together products from across Cisco's portfolio. Products referenced in this paper include:

- Cisco AnyConnect Secure VPN
- Cisco DNA Center network controller and management dashboard
- Cisco Secure Endpoint cloud-delivered, advanced endpoint detection and response (EDR)
- Cisco Meraki MX, a multifunctional security and SD-WAN enterprise appliance
- Cisco Meraki Systems Manager, Cisco's endpoint manage ment solution
- Cisco Webex, the calling, conferencing and meeting soft ware
- Cisco Identity Services Engine (ISE), which offers zero-trust security for the workplace
- Cisco Umbrella cloud-delivered security
- Cisco Catalyst Switches

More detailed information about these products can be found in the Appendix.

How PeerSpot Members Are Using Cisco Hybrid Work Solutions

PeerSpot members are putting the Cisco hybrid work solution to work in a variety of use cases. For example, the founder and president of AAnnex, a comms service provider, uses Cisco Web to handle remote meetings. He shared, "If we need to have international meetings or client meetings, we use this solution. We also use it if we need to share desktops remotely or remotely control a customer's environment. We use it to record calls as well."

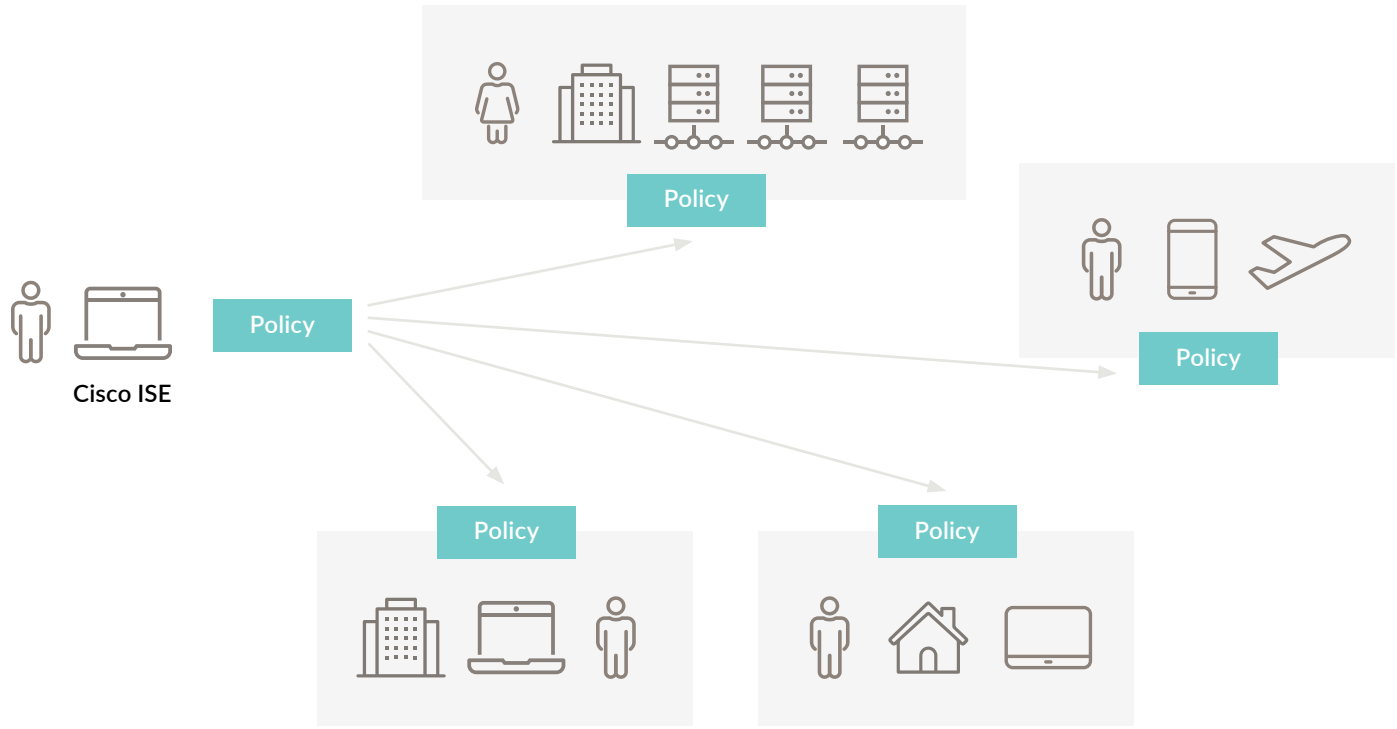


Figure 1 - Hybrid work use cases.

> "We could establish a network between two sites, and that has improved and increased communication and productivity."
>
> Read review »

Cisco AnyConnect Secure Mobility Client enabled people at a software company with more than 5,000 employees to "work from home without security concerns," according to their senior specialist: concept development. Cisco DNA Center has been useful for a managing director at Allot Group, a comms service provider, who relies on the solution in day-to-day operations, especially post-pandemic, because, as he put it, "The majority of our customers have to work from anywhere. It's not just work from home, it's work from anywhere." Figure 1 shows these use cases.

He added, "Due to this work from anywhere concept, the traditional silos of a network for the data center architecture, and managing everything from anywhere, and having that single integrated dashboard for each and every activity while being able to correlate those activities in line with a business objective, has been very well addressed by Cisco DNA."

"By using the VPN, we can connect remotely," said a director who uses Meraki MX. "We have two offices, and we could connect them through the VPN. We could establish a network between two sites, and that has improved and increased communication and productivity. Our remote site is able to access the server remotely."

Keys to Making Hybrid Work, Work Better

The IT department and security team are on task to make hybrid work a success—now and in the future. This responsibility requires them to have solutions that can handle security for employees, the organization, and its digital assets regardless of pressures of hybrid work.

IT must also support the kind of flexibility and collaboration that employees need to be effective in the hybrid mode of working. Flexibility is the defining premise of hybrid work. The workforce is empowered to demand flexibility in work models, which challenges IT and human resources (HR) organizations alike. Flexible work models naturally introduce new security challenges. They increase the need for better visibility into endpoints and networks. After all, one can't fix what one can't see. Flexible work models also stress IT management capabilities.

Flexibility and Collaboration

Given the importance of flexibility in hybrid work's remote work scenario, the systems that support flexible work models must themselves be flexible—able to adapt to new circumstances with little warning. In this context, a senior specialist, e-transformation services who uses Webex at a tech services company with over 200 employees, said, "You can configure whatever you want in great detail. It's very flexible."

Businesses that want to succeed with hybrid work must enable collaboration by team members who might be working from any number of locations. This, too, requires flexibility in the toolset. The founder & CEO at a tech services company praised Webex in this regard, saying, "My advice to anybody who is considering Webex is that it is a great tool for having meetings and collaborating with customers, suppliers, and employees." A consultant - risk and compliance who uses Webex at a tech services company similarly noted, "The solution makes it easy for us as a team to collaborate remotely."

For a director who uses Webex at a financial services firm with over 200 employees, the collaboration advantage came from one-click calling, which makes things easier for his people. He said, "You click, and it automatically dials in to the meetings without pressing additional buttons. It's easy for people who aren't on Webex. That was helpful."

> **"You can configure whatever you want in great detail. It's very flexible."**
>
> Read review »

"Easy to use, flexible, and simple to set up"

Read review »

A central services engineer who uses Meraki MX at Liberty Technology, a tech services company, spoke to the synergy of Cisco remote work products when he said, "Webex and Meraki kind of work together. That is the whole layering thing. Webex is for your team collaboration. We use analytical data from WebEx Control Hub and Meraki to figure out issues with calls. We have to route it the right way, then figure out if the ISPs are giving us packet loss. Almost anything goes out to the Internet 100 percent works with Meraki because you have to troubleshoot the ISP, and Meraki is how you do that."

Several users of Cisco Catalyst Switches commented on the product's flexibility, which helps support hybrid work use cases:

- "Helps us connect drivers and desktops, the expandability provides flexibility." - System administrator at a software company

- "Easy to use, flexible, and simple to set up." Network engineer at a retailer with over 10,000 employees

- "Good scalability with very nice stability and good flexibility." - Junior network engineer at a tech services company

- "These switches are flexible and user-friendly." - CEO at a construction company

- "The product is extremely flexible." - IT Manager pan India at Escon Elevator Private Limited, a tech company with over 200 employees

Security

Remote access is not new or unique to hybrid work. However, the scale and scope of hybrid work use cases put pressure on existing security solutions. Cisco Umbrella offers a solution by adapting to the new requirements of hybrid work. According to a network operations center (NOC) lead who uses Cisco Umbrella at a tech services company, "The primary use case is for endpoint users who are not working on our office premises. They are remote employees who are roaming so they are not within our protected zone. There can be vulnerabilities if they are browsing content and there is malware included on those web sites."

Umbrella allows monitoring on remote devices. "We can block those sites," the user added. "We can also block applications which we would like not to allow to be running in the organization." This user also deploys Umbrella to protect users from malware phishing through email and the websites they are browsing. In their case, Umbrella is a solution for DNS (Domain Name System) protection, filtering and security.

Further to the issue of secure web browsing by remote, the chief executive officer of Cynexlink, a tech services company, shared how Cisco Umbrella acts as web filtration combined with security. He said, "It's important for end users to have some sort of protection when they're browsing the internet and this product does that. Before it lets you go, it filters and gives you the okay to move forward with the website you're looking for." His team manages about 1500 endpoints under Cisco Umbrella.

"It's important for end users to have some sort of protection when they're browsing the internet and this product does that."

Read review »

Easy for us as a team to collaborate remotely

Secure system access is important for hybrid work, but employees must only be able to have remote access to resources for which they have permissions. As an accounting executive at a tech services company commented, "The ISE product is used to make sure that folks can get access to the application servers that they need to get access to, let's say for accounting and another group like sales and marketing, they would have no business accessing each other's servers, those apps. So, you would set up a policy that allows accounting to do what they have to do whether they're remote or on campus and then the sales and marketing folks could never access that. They are totally blocked. It's a virtual firewall, basically."

The policy definition and enforcement can be quite granular, as the Accounting Executive further remarked. He said, "The way the ISE works is you can get into defining. Let's say, in my case, I've got a Windows laptop and I've got an Apple product and those have unique identifiers, unique back addresses. It would say that this in my profile so I could get to those apps with either device, 24/seven. That's how granular the ISE or these NAC Solutions can get. That you have to have that same device."

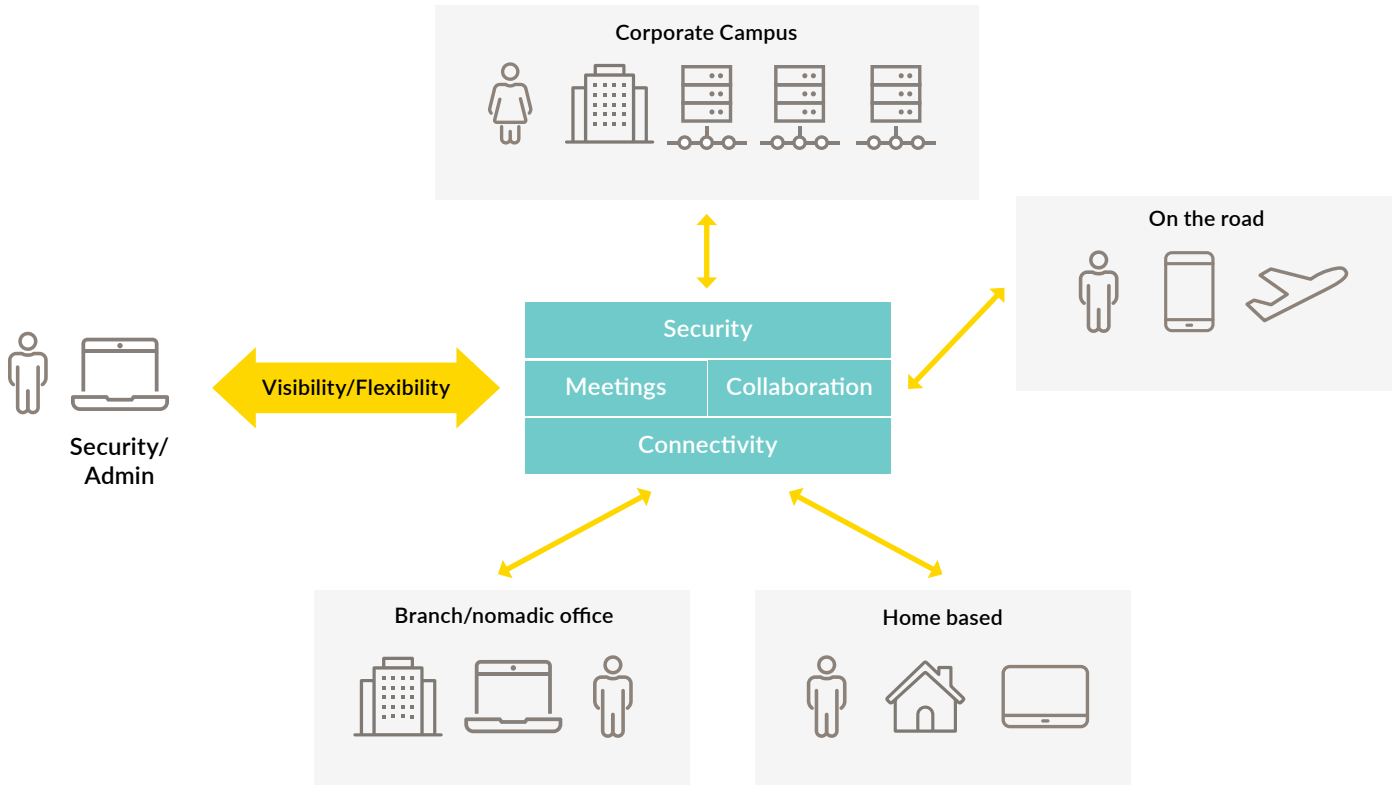
Passcode policies are what stood out for the president of virtualtechsolutionsusa.com, a tech services company. Cisco Meraki protects their devices and employee data, controlling usage with a passcode policy. He elaborated, saying, "Every device will have a passcode policy. This restricts employee access to, for example, app stores, gaming, and so on during work hours." He added that a passcode policy can restrict access and enable device restrictions to stop people from being able to use cameras. He said, "You can allow screen capture, automatic sync when roaming, and the use of a virtual assistant, or you can actually shut all these things down as well."

Manageability

Having employees working in a variety of on- and off-site scenarios makes it hard to conduct standard device and network management tasks. Management solutions have to be able to handle new, diverse workloads—while delivering great end user experiences and facilitating productive IT operations. Hybrid work makes these needs more urgent than ever. With not everyone in the same place, IT support and user experience are of paramount importance. And, the nature of hybrid work tends to make this challenging to achieve. Cisco solutions make a difference in this regard.

A technology manager at Advanced Integrated Systems, a tech services company, explained, "Cisco ISE offers one central point to create different policies for different groups of users and enforce policies to each entity regardless if it's connected to the network through wired or wireless network devices." Figure 2 depicts this capability.

Figure 2 - Centralized policy definition and administration.



> "It integrates very well with network devices to control port configuration services authentication and authorization"
>
> Read review »

For his team, Cisco ISE provides more mobility and wireless-wired converged network. He added, "Also it integrates very well with network devices to control port configuration services authentication and authorization. ISE also integrates with DNA center and Stealthwatch to enable the customer to have an SDN (software defined network) fabric." On a related front, a senior network engineer at a tech services company with over 200 employees shared, "In terms of endpoint end users, DNA is collecting assurance and telemetry from several thousand. It's being fully utilized."

Centralization also stood out to this user, who said, "Rather than having to log into the individual switch DNA center, you can basically run your commands, run your troubleshooting, all from DNA, and attempt to remediate the problem." He then noted, "DNA center is very capable of being able to address and identify the issue, suggest remediation steps, run remediation, run commands against a switch to check the proper connectivity for example, and also address all our remediation steps that the IT person could take."

"Meraki MX is great for WAN networking, e.g., when you have multiple ISPs at the one site or you have a large network that expands across a large physical area, like across a state or county," said Liberty Technology's central services engineer. Wide Area Networks (WANs) are an essential element of hybrid work in geographically distributed organizations. He then related, "You use it to have a seamless VPN that you are not managing on devices or if you have a client VPN that needs to be easily integrated into the firewalls."

Visibility

PeerSpot members found that the Cisco hybrid work solution provided the kind of visibility that's needed for delivering an effective hybrid work environment. "It gives us visibility with minimal intrusion," said an IT manager who uses Cisco Secure Endpoint at van der Meer Consulting, a construction company. A senior network engineer at High Frequency Trading, a tech services company, concurred, saying that Cisco Catalyst Switches are easy to use and provide good network visibility. A VP of IT who uses Cisco ISE at a tech services company simply said, "Provides visibility of traffic, and is easy to use."

"At the end of the day, AMP will feed both data feeds and give you good visibility into all your traffic, whether it's leaving your network, coming into your network, or going across your network," said a CIO who uses Cisco Secure Endpoint at Per Mar Security Services, a security firm with over 1,000 employees. He went on to explain what he found most valuable about the solution, sharing, "For the endpoint, Cisco gives us good clarity about what our endpoints are actually doing. So, when we get bad actors into the network, we get quick visibility into which devices are compromised. We're able to see hashes, and the like, all the way down to the client and we get that visibility because of AMP."

> **"It gives us visibility with minimal intrusion"**
>
> Read review »

Visibility from around the globe

For this user, further visibility advantages arise from the integration of the Cisco Threat Response feature with products like Cisco Email Security, Cisco FirePOWER, Stealthwatch, Talos, Threat Grid, Umbrella, and third-party solutions. “Talos is out there as the guiding force, applying visibility from around the globe, and the insights that it gains, and then feeds back into all the security platforms,” he said. “Threat Grid lets us see and track hashes with the forensics that we get. That’s where Umbrella and AMP come into play, and having those agents out there running on endpoints and feeding it all the way back up the stack and giving us visibility into all our north-south traffic through the network. That is important.”

Conclusion

Hybrid work is here to stay, though it will inevitably evolve into a different form than it is taking today. For IT, this means implementing solutions that provide a flexible, adaptable foundation upon which organizations can address the continued evolution of hybrid work. Operationalizing such an idea requires solutions that enable security and manageability for devices and people who work from a variety of locations. It means having visibility into networks and endpoints. Flexibility is critical. The Cisco hybrid work solutions meet these criteria. They are robust and flexible enough to support hybrid work in all its many, ever-changing forms.

Appendix: Product descriptions

• **Cisco AnyConnect Secure** — A secure VPN that offers remote workers frictionless, highly secure access to the enterprise network from any device, at any time, in any location while protecting the organization.

• **Cisco DNA Center** — A powerful network controller and management dashboard that helps users to manage and troubleshoot their networks. It offers guided workflows specific to each user's job role in NetOps, AIOps, SecOps, or DevOps.

• **Cisco Secure Endpoint** — Cloud-delivered, advanced endpoint detection and response (EDR) across multi-domain control points to rapidly detect, contain, and remediate advanced threats. The solution offers simplified investigations, integrated XDR capabilities and threat hunting.

• **Cisco Meraki MX** — Multifunctional security and SD-WAN enterprise appliances with a wide set of capabilities to address multiple use cases–from an all-in-one device. Organizations of all sizes and across all industries rely on the MX to deliver secure connectivity to hub locations or multi-cloud environments, as well as application quality of experience (QoE), through advanced analytics with machine learning.

• **Cisco Meraki Systems Manager** — Cisco's endpoint management solution, which supports a variety of platforms, allowing for the diverse ecosystem often found in today's mobile centric world. This places Systems Manager in prime position to alleviate the concerns of security teams in various industries, empower teachers to run their digital classroom, and ease the burden of enterprise IT teams with distributed sites. Systems Manager offers centralized, cloud-based tools for endpoint management with far-reaching scalability for growing organizations.

• **Cisco Webex** — Calling, conferencing and meeting software that minimizes interruptions and let everyone participate, equally. Messaging features keep work flowing in between meetings with rich messaging, secure file sharing, and whiteboarding for continuous teamwork. Other features include polling, events, whiteboarding, and asynchronous video.

• **Cisco Identity Services Engine (ISE)** — The centerpiece in zero-trust security for the workplace, enabling a dynamic and automated approach to policy enforcement that simplifies the delivery of highly secure network access control. ISE empowers software-defined access and automates network segmentation within IT and OT environments.

• **Cisco Umbrella** — Flexible, cloud-delivered security when and how the user needs it. It combines multiple security functions into one solution, so users can extend protection to devices, remote users, and distributed locations anywhere. Umbrella is the easiest way to effectively protect users everywhere in minutes.

• **Cisco Catalyst Switches** — Campus LAN switches for access, core and distribution use cases.

About PeerSpot

PeerSpot (formerly IT Central Station), is the authority on enterprise technology. As the world's fastest growing review platform designed exclusively for enterprise technology, with over 3.5 million enterprise technology visitors, PeerSpot enables 97 of the Fortune 100 companies in making technology buying decisions. Technology vendors understand the importance of peer reviews and encourage their customers to be part of our community. PeerSpot helps vendors capture and leverage the authentic product feedback in the most comprehensive way, to help buyers when conducting research or making purchase decisions, as well as helping vendors use their voice of customer insights in other educational ways throughout their business.

www.peerspot.com

About Cisco

Software is at the heart of the network's transformation to the Digital Age. Cisco is a leader in software development and has the industry's broadest ecosystem, with more than 300 development partners. Piecemeal, non-integrated solutions defeat the objective of end-to-end digitization, and only Cisco with its Digital Network Architecture and partner ecosystem can help you visualize and develop a holistic digitization approach to it. All while preparing for the security vulnerabilities that arise with the multitude of people and devices now connected to the network.