

Secure Networking for the Hybrid Workplace

Overview

For most of us, the future of work is distinguished by a more geographically dispersed, highly engaged, and collaborative workforce. This future is very dependent on workers getting access to the distributed digital resources and services they need to do their

jobs and collaborate effectively. A secure, agile network has never been more important. Your network needs to support the secure user experience employees require when accessing applications dispersed across multiple cloud and on-premises environments.



Figure 1. The hybrid workplace is becoming the new normal

Source: [Global Workforce Survey: The Rise of the Hybrid Workplace Report](#), 1 Oct 2020

Benefits

Recent events are encouraging organizations to adopt a hybrid model that blends a safe return to the workplace with work from home. With Cisco's secure networking solutions, you can help your workforce be protected, productive, and engaged anywhere they choose to work.

- **Secure user experience:** Secure and optimize the user experience for applications located anywhere
- **Workplace safety:** Support the health and wellness of employees as they return to the workplace
- **Operational efficiency:** Use automation and insights to simplify operations and optimize the user experience
- **Business resilience:** Enhance IT's ability to quickly respond to business imperatives and disruptions
- **Scalable platform:** Adopt a scalable hardware or software platform that accelerates the transition to hybrid work in a simple and agile manner



“As digital enterprises move from hybrid workforces by circumstance to hybrid by design, we will see the evolution of both physical and digital workspaces, driving innovation as well as productivity, a better worker experience, and business resiliency.”

Source: IDC FutureScape: Worldwide Future of Work 2021 Predictions

Solutions

How can Cisco help? We can provide you with a complete networking platform for all your organization’s hybrid workplace and business resilience requirements. Cisco® network solutions enable a safe return to the workplace, secure work from home, and anywhere access to multicloud applications.

[Trusted workplace networking](#)

Enable a safe and secure return to the workplace by monitoring social density, securely onboarding users and things, and helping ensure that employees can be protected in their environment.

- **Secure access:** Make your IT operations more efficient, your network more secure, and your user experience more consistent across wired, wireless, and VPN infrastructure with our advanced SD-Access solution for automating user policy and network access.
- **Smart building services:** Enable smart building services by simplifying the onboarding of IoT devices such as cameras, heat sensors, and smart lighting. Use policy automation, AI Endpoint Analytics, and microsegmentation to simplify security, together with Cisco Universal Power over Ethernet (Cisco UPOE+) and Cisco Multigigabit technologies to simplify connectivity.
- **Social density monitoring:** Use cloud-based Cisco Spaces applications in combination with advanced Wi-Fi data telemetry and Cisco Meraki® cameras to monitor social density thresholds in buildings. Provide real-time alerts and respond to incidents with proximity reporting.

Getting started

How can you get started?

- Find out more: www.cisco.com/go/networkresiliency
- Read: [e-book](#)

Secure remote workforce networking

Empower employees to work productively and securely by extending enterprise network connectivity to remote workers at home and anywhere. Going beyond traditional VPN connectivity, these solutions extend corporate policies, security, and visibility, making life easier for remote employees and IT administrators.

- **Cisco Remote Workforce Wireless solution:** Cisco access points offer plug-and-play provisioning and policy automation and allow your remote employees to easily and securely connect to the corporate network without setting up a VPN.
- **Cisco Remote Workforce Routing solution:** Extend a uniform enterprise SD-WAN to the home and remote workforce. Extensive cloud integration delivers a consistent and optimal application experience. Cloud-delivered Secure Access Service Edge (SASE) architecture provides unified security and compliance. A highly visualized centralized management dashboard automates deployment, configuration, and troubleshooting in an agile and scalable manner. Flexible hardware and software endpoints accelerate the transition to a hybrid workforce wherever and whenever it is needed.

Secure multicloud access

Enable the adoption of multicloud strategies by allowing your users to consistently and securely access public Infrastructure-as-a-Service (IaaS), Software-as-a-Service (SaaS), and on-premises applications across hybrid workplace environments.

- **Cisco SD-WAN:** With Cisco SD-WAN solutions you can deliver efficient access to cloud applications in multicloud SaaS and IaaS environments. They also help you protect against security vulnerabilities.
- **Cisco SD-WAN Remote Access (SD-WAN RA):** Integrate remote access functionality into the SD-WAN fabric to extend all the benefits of Cisco SD-WAN to the remote workforce. Remote workers can simply leverage existing remote-access clients (including Cisco AnyConnect®, Windows or Apple OS native clients and hardware-based routers such as the Cisco Catalyst™ Wireless Gateway) to access the nearest Cisco SD-WAN edge device, regardless of their location and devices.
- **SASE:** Cisco SASE solutions bring together Cisco SD-WAN and Cisco Umbrella® cloud-based security in a single, cloud-native service to help secure access wherever users and applications reside.