6 Critical Considerations for Secure Hybrid Work

The new normal is that companies must evaluate how to preserve business processes while acknowledging that hybrid work is here to stay. Secure hybrid work is achieved when security and connectivity are fast, easy-to-use, and can protect transactions wherever people and data go—all while ensuring an employee has the same, productive user experience they would when using technology in a traditional corporate office.

Here are six critical considerations to make sure you're properly securing your hybrid workforce.

Ensure Your Security Applies Zero Trust Principles

Attackers are following businesses to the cloud because that's where most data is stored. And with the hybrid workforce being able to access that data from a number of devices and networks, the notion of "implicit trust" is no longer viable. Zero trust is a shift from trust but verify to verify then trust, built on the concepts of context-aware least privileged access and continuous assessment.

Click here to dig in a little deeper on Zero Trust

Don't Lose Sight of the User Experience

The right security solution should take each of the previous considerations into account, but needs to do so in a way that has minimal impact on the hybrid work user experience. Avoid security solutions that impose high latency penalties or force traffic to take inconvenient detours. Additionally, security controls shouldn't hog system resources or require a number of extra clicks.

Read more:
Security Doesn't Have to Slow Down Network Performance

Design Your Security to Maximize Visibility and Control of Your Cloud-Centric Environment

Protecting your data, systems, and devices in a hybrid work environment requires visibility and control of cloud and SaaS applications. (The average enterprise uses over 2,415 SaaS applications, the vast majority of which are unmanaged—i.e. "Shadow" IT.) The ability to see, guide, and control the activity of everyone in the business dramatically improves risk awareness and detection.

Click here to read our blog

Design for All Data Protection Use Cases Across Web, Cloud, Email, Private Apps, and Devices

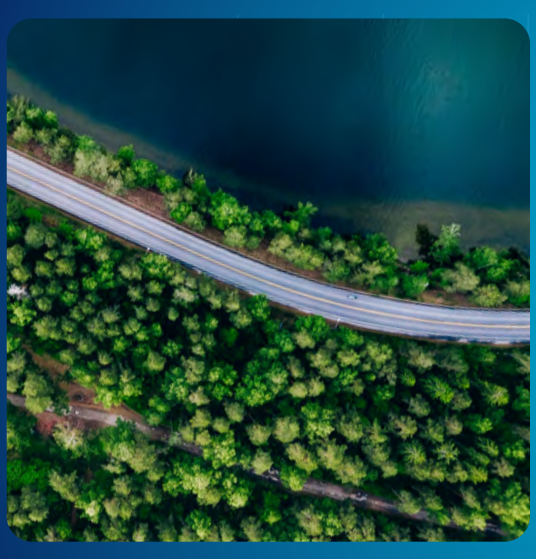
Hybrid work has dissolved the notion of a security perimeter and expanded the enterprise beyond on-prem; your security has to make considerations for traffic from the web, cloud, private applications, and devices. CASBs, SWGs, ZTNA and all other aspects of a Security Service Edge (SSE) architecture address data moving and stored across all of these vectors.

Read the Cloud Data Protection White Paper

Design Your Security Around Context

Hybrid work dramatically complicates the different ways users can interact with applications and data, meaning that security needs to have far greater contextual awareness when making access and policy decisions. Security must constantly monitor traffic after access is granted, conduct a contextual analysis of sessions, make decisions informed by third-party risk intelligence, detect changes in risk profiles, and neutralize dangerous actions.

Click here to learn more about the Netskope Cloud XD Platform



Consolidate Vendors to Enhance Your Security Effectiveness—and Lower Costs

The average enterprise employs 76 security tools. SSE won't replace every one, but you won't need the complexity and headaches of a patchwork security environment with scores of vendors. A unified, single-vendor comprehensive suite replaces poorly coordinated legacy security solutions. Merged capabilities simplify management and administration, ensure consistent policy enforcement, streamline traffic processing, and improve total cost of ownership.

Find out more about what Netskope Intelligent SSE can do for you!

Netskope, a global cybersecurity leader, is redefining cloud, data, and network security to help organizations apply Zero Trust principles to protect data. The Netskope Intelligent Security Service Edge (SSE) platform is fast, easy to use, and secures people, devices, and data anywhere they go. Learn how Netskope helps customers be ready for anything on their SASE journey, visit netskope.com.