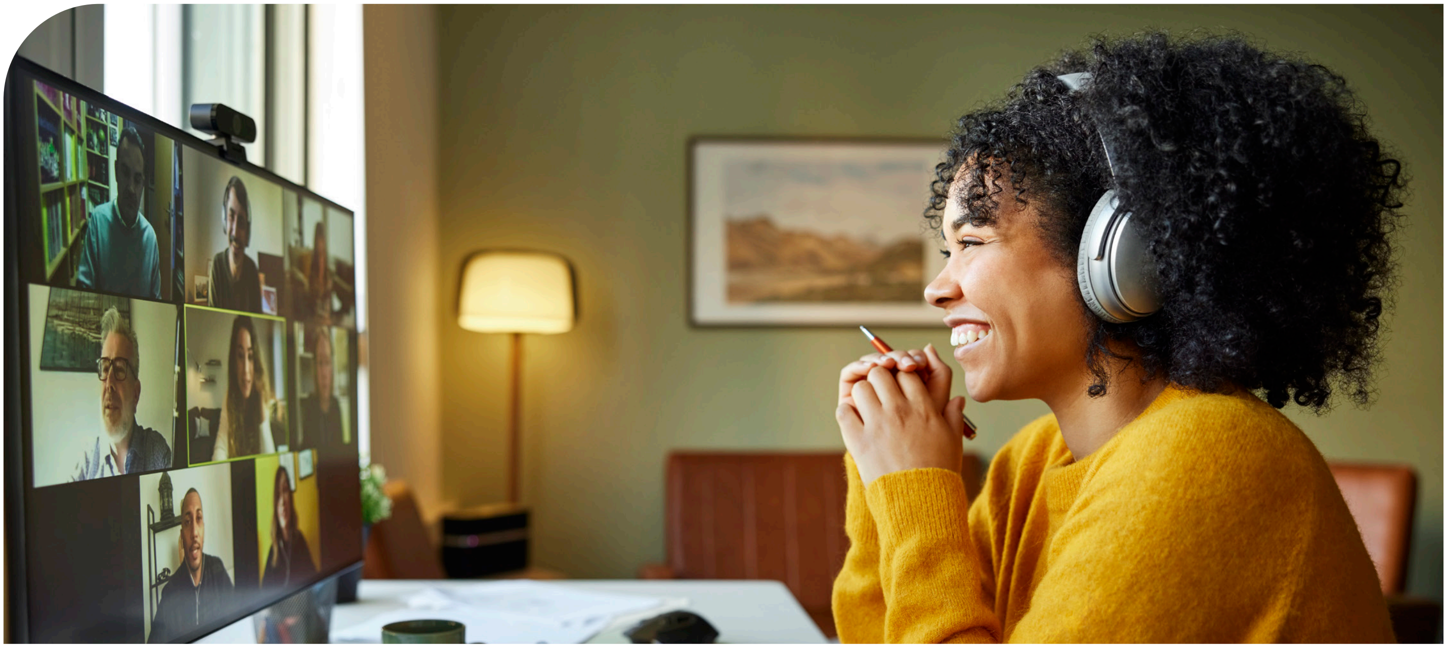
unisys



Use case

Unisys Secure Access Solution

Zero Trust security for your hybrid workforce

The increasing need to work from anywhere - as well as the desire to implement a Zero Trust security strategy-requires government and businesses to rethink how they secure their users - where ever they are. Business continuity and contingency planning demands that you provide, anytime, anywhere secure access to vital resources, data, and applications. Providing remote access via traditional virtual private networks (VPNs), however, increases risk and expands the attack surface. And hackers are taking advantage of this weakness to infiltrate company networks and steal information.

Traditional VPNs have been part of many organization's security strategy for years. Perimeter-based VPNs are deployed to provide remote access to corporate resources. The challenge is that once users are connected, they have access to the entire network, putting sensitive data at risk. VPNs fail to provide the connectivity and the security that companies need to ensure business continuity and to implement a Zero Trust security strategy. They are vulnerable to man-in-the-middle attacks, lack the granular control that is crucial for securing access over untrusted networks, and allow hackers lateral movement once inside a private network. In short, VPN services are too lenient and fail to protect your business in a world where data and applications must be made available beyond your organization's perimeters.

VPNs leave you at risk for a breach because they:

- **Do not** easily provide granular control, especially on untrusted networks
- **Do not** allow for scalability to tens of thousands, often because VPN concentrators have significant limitations
- **Do not** prevent hackers who pass a VPN gateway from engaging in lateral movement inside the private network
- **Do not** encrypt data from the VPN gateway to internal assets, making data on the wire vulnerable to man-in-the-middle attacks

Put simply, VPNs do not deliver the Zero Trust security that is critical to provide connectivity and prevent cyberattacks in the flexible-location business model. Rather, they represent a single point of failure within any organization. Even when VPNs are working at their fullest potential, they leave your network vulnerable.

Anytime, anywhere connectivity with Unisys Secure Access Solution

The Secure Access Solution is a proven, end-to-end solution that secures users in the office, at home and when traveling.

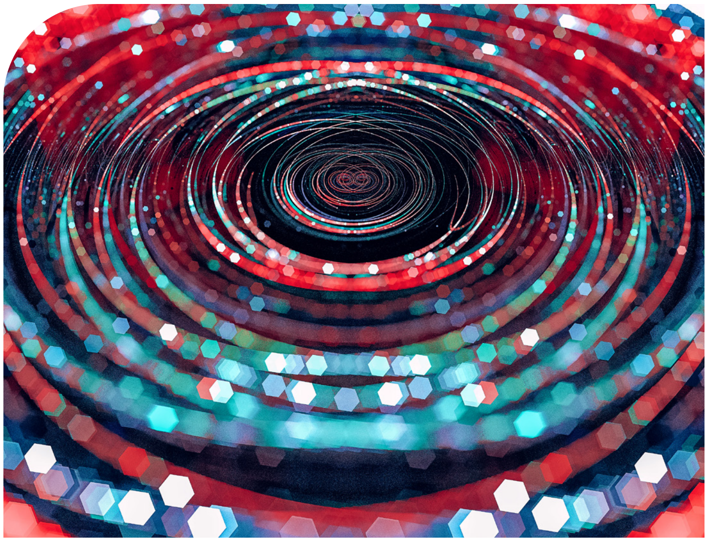
It guarantees that users only have access to the data and applications they need – not the entire network. It rigorously protects your organization against the onslaught of bad actors seeking to exploit your environment. And, it delivers Zero Trust security by:

- Providing scalable, secure access to users regardless of the number of users or their location, even over untrusted networks
- Granting users access only to what they need, not the entire network
- Extending the operational reach and access of your workforce
- Reducing your reliance on vulnerable remote work solutions such as VPNs
- Enabling you to handle load, scale, and security at the level your organization needs
- Encrypting data-in-motion to prevent man-in-the-middle attacks
- Reducing the attack surface without impeding authorized access

The Secure Access Solution can be deployed completely in your environment or as a managed service - which ever works best for you. Either way, you can deploy Secure Access quickly and cost effectively, protecting your business while supporting contemporary remote work options.

Even better, a Secure Access deployment can serve as a platform to re-imagine your network architecture, increasing your security and reducing your operational costs though the elimination of private network links. We've done this as part of our Zero Trust implementation at Unisys, and we'll show you how you can as well.

With the Secure Access Solution, you can position your business for success – today and every day.



Unisys Secure Access is powered by Stealth™, which is identity-based segmentation software that is the foundation of a Zero Trust security strategy. Stealth simplifies and improves network security even in hybrid/complex IT environments and replaces the traditional VPN attack surface.

- Stealth delivers identity-based micro-segmentation by creating cryptographic communities of interest (COIs) that limit access to the other users, applications, and data.
- Stealth users enjoy "wifi anywhere" security with a consistent, seamless user experience everywhere - at home, in the office or on the road.
- Stealth employs and manages hyper-secure IPsec tunnels, leveraging military-grade encryption to strongly protect data from end-to-end.
- Stealth provides orchestration and deployment that is highly-automated and centrally-managed so that, as your security policies evolve, changes can be made once and propagated instantly across the enterprise.

Learn more about how we can quickly secure your remote work force at www.unisys.com/Security.

unisys

unisys.com