Unisys Always-On Access™ Powered by Stealth™

Secure Your Remote Workforce for Optimal Productivity and Cyber Resiliency

The increasing trend towards remote work and hybrid work requires government and businesses to rethink how they secure their remote users, including employees, contractors and supply chain partners. Business continuity and contingency planning demands that you provide always-on, anytime, anywhere access to vital resources, data, and applications. Expanding remote access via traditional VPNs, however, increases risk and expands the attack surface. And hackers are taking advantage of this shift to infiltrate company networks and steal information.

Traditional virtual private networks (VPNs) have been an essential part of an organization's security strategy for years. Perimeter-based VPNs are deployed to provide secure, 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 both the connectivity and the security that companies need to ensure business continuity. They are vulnerable to man-inthe-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.

In the midst of this transition, Unisys Always-On Access™ powered by Stealth™ is a proven, end-to-end security solution that has been securing remote workforces for years – even for users relying on untrusted devices and networks. And the best news of all is that through the Unisys Always-On Access capability, your organization can replace vulnerable VPNs with Zero Trust security now, at the exact moment you need secure access the most.

Secure Your Remote Users With Unisys Always-on Access Powered by Stealth

Unisys Unisys Always-On Access guarantees that employees, partners, and the entire supply chain 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 the current crisis. Unisys Always-On Access robustly protects your organization by:

- Providing scalable, secure access to users regardless of user quantity or 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

With Unisys Always-On Access powered by Stealth, you gain both speed-to-market and speed-to-security since you retain your entire existing infrastructure and applications. There is no need for an expensive and time-consuming "rip and replace" effort – you can deploy Unisys Always-On Access quickly and cost effectively, securing your business while supporting contemporary remote work options.

Through Unisys Always-On Access, you can position your business for success – today and every day.

Unisys Always-On Access powered by Stealth establishes a software defined, identity-based segmentation that is the foundation of a Zero Trust security strategy. By doing so, Stealth simplifies and improves network security even in hybrid/complex IT environments and replaces the traditional VPN attack surface.

- Stealth overlays every corner of your organization's computing environment with one holistic, consistent, and unwavering security policy – encompassing desktops, servers, cloud, mobile, Kubernetes containers, and IoT
- Stealth delivers identity-based micro-segmentation by creating cryptographic communities of interest (COIs) that limit access to the other users, applications, and data also assigned to the COI
- Stealth employs hyper-secure IPsec tunnels, leveraging military-grade encryption to strongly protect data from end-to-end
- Stealth provides orchestration and deployment that are highly-automated and centrally-managed so that, as your security policies evolve, changes can be made once and propagated instantly across the enterprise

Secure Your Remote and Hybrid Workforce

Learn more about how we can quickly and securely enable your remote workforce while reducing your risk exposure and allowing your business to thrive at www.unisys.com/Security.

Request an Assessment at www.unisys.com/contact-us.

For more information visit www.unisys.com