Four reasons to kill the VPN: security, speed, simplicity and savings

The enterprise network has moved from tightly-bound to boundless

Four reasons to kill the VPN: security, speed, simplicity and savings

Zero Trust security and virtual private networks

The network perimeter is changing. IT environments encompass multiple topologies, including on-premise hardware, private clouds, and public clouds. Companies share applications and data with dozens of partners and vendors. Businesses are extending their operational reach and access to a remote workforce that is itself dynamic and elastic in nature. Employees, vendors, partners, customers, and other stakeholders are constantly logging in from different devices, using different connections, and working from different locations. CISOs, CIOs, and CSOs are being asked to secure identities and devices across unknown and untrusted shared common infrastructure.

In such a world, the enterprise network has moved from tightly-bound to boundless. Consequently, whatever protection Virtual Private Networks (VPNs) afforded to an enterprise's data and critical assets has been completely destroyed. Businesses need a new and better way to secure their "crown jewels." That is found in a Zero Trust security approach which controls access to resources based on user identity, continuously verifying users and limiting network access based on the concept of least-privilege.

While the Zero Trust concept emerged in the last decade or so, Unisys has been deploying Zero Trust since 2006 with the inception of the Unisys Stealth® microsegmentation technology. Stealth™ was originally developed to satisfy a U.S. government need to share sensitive and classified information over untrusted networks. Today, Stealth is used to power the **Unisys Secure Access Solution,** which provides users secure, scalable access only to the data and applications they need - not the entire network.

Security: eliminating VPN vulnerabilities

To better understand why Zero Trust calls for the eliminations of VPNs, visualize your enterprise's network as a house and a VPN as a door. That door opens for anyone who has a key – or who can jimmy the lock. Obviously, the door is where burglars are going to concentrate their efforts. Practically speaking, it is not that hard to break in. Plus, once they get through the door, there are no further barriers to navigate. They are "home-free" to move where they want and steal what they want.

In like manner, hackers love VPNs because they are relatively easy to crack. They are a door into your network. Once a VPN is compromised, the attack can propagate laterally and at a great pace from server to server within the data center, with no security controls in place to stop the spread. VPNs therefore represent a single point of security risk for the network.

VPNs were designed to protect the network perimeter at a time when that perimeter was still defined and finite. When only a handful of "doors" into a network existed, they could be monitored and maintained. But the expanding network means doors – and attack vectors – have grown exponentially. It is next to impossible to ensure that all the doors are locked, or to verify whether everyone coming through those doors has a right to do so.

Zero Trust, in contrast, can be visualized as a house with no doors. The exterior is a solid brick wall. With no door, a hacker has to hammer away at a brick to remove it. But, because the network is protected by microsegmentation, the most a hacker can get is ... a brick. Nothing more. Access to the entire house is never possible. Why? Because there is no "inside" to this house: microsegmentation has converted an "open floor plan" house into a solid cube of discrete bricks.

But there is more to the Secure Access Solution, than even that. Suppose a hacker succeeds in loosening a brick. Stealth has guard dogs on watch for exactly that. They instantly surround the hacker, preventing him from touching another brick. They also stop him from leaving the premises with the brick he managed to loosen. This is **dynamic isolation**: Stealth isolates critical data and systems from rogue users to contain an attack in less than ten seconds, preventing data exfiltration and giving security personnel time to investigate an attack.

Businesses need a new and better way to secure their "crown jewels."

VPNs represent a single point of security risk for the network.

VPN encryption typically utilizes AES-256 bit encryption schema, employing the same basic crypto chassis as standard TLS and SSL connectivity. This is simply not enough for today's more sophisticated threat actor and contested operational environment. Stealth, by contrast, leverages standard AES-256 as the basis for an enhanced crypto chassis, employing additional modules to increase protection levels commensurate with National Security standards, making it able to handle the most sensitive data on the face of the earth. With this level of encryption, data in motion is fully protected and ready for worldwide use today, out of the box.

Speed: deploying at the critical moment

Achieving stronger security is not the only advantage of eliminating a VPN from Zero Trust deployment. Another major benefit is speed. VPNs, by their nature, are time-intensive to deploy. There are countless scenarios to consider, users to assess, and rules to be written. But for Zero Trust, if you select the right approach, the time required for deployment drops dramatically. In the case of the Secure Access Solution, that time is counted in weeks, not months. Installation is easy – driven by the push of a light-weight installation package onto a user's device. In this way, you can roll out a key element of Zero Trust literally overnight to thousands of users.

From the user's standpoint, they automatically have a secure connection going forward. Nothing else changes: the user does not have to follow any instructions or configure their device in any way. The Secure Access Solution is completely transparent to the end user. In fact, the only change users will notice is that it is easier than ever to connect to the network and get their work done.

Simplicity: streamlining security management

Complexity vs. simplicity is another area where VPNs stumble. VPNs are synonymous with complexity since they are notoriously difficult to design, manage, and maintain. For a VPN to provide a reasonable level of access control, you must keep detailed and current documentation (a near impossibility with today's rapidly-expanding network), configure policies appropriately for different geographic regions, and address compatibility problems with other types of software.

Now, add in a hybrid workforce that could number into the tens of thousands. For most systems, each time a new VPN is added or a new user is added to a VPN, a new firewall rule set needs to be written, burdening access control lists. Ensuring that each of those rule sets is up to date at all times is challenging given the dynamic nature of the workforce, the network, and the business. Before long, complexity goes through the roof and security goes through the floor.

Zero Trust, when implemented correctly, brings simplicity by streamlining security management across networks, users, and devices. With the Secure Access Solution security policies are driven by the identity of the user or device in-line with Zero Trust security principles. From a management perspective this means that even when the underlying infrastructure changes, the security policies remain consistent.

The Secure Access Solution delivers simplicity in other ways as well. For instance, there is a seamless user experience, whether in the office, at home or traveling. In fact, users can securely "WiFi Anywhere" without invoking a VPN. There are also options to deploy Secure Access as a Managed Service, further streamlining both implementation and on-going management.

Savings: maximizing operational resources

Finally, there is the consideration of cost. Again, A Zero Trust deployment that eliminates the use of a virtual private network will save you money in the short- and long-term, as shown in this table:

VPN	Zero Trust with Unisys / VPN Elimination
Requires a dedicated team to manage the complexity of the VPNs	Does not require a dedicated team, freeing up headcount for higher value tasks
Uses expensive hardware	Saves money with software-only overlay approach
Has compatibility issues with other software	Integrates seamlessly with existing security tools, avoiding the cost and disruption of a "rip and replace" effort
Adds costs with new users, new services, and new VPNs	Scales easily, without additional costs for new users, new applications, or new services

Making the move to Zero Trust

Increased security, speed, simplicity, and savings. That is the bottom line when it comes to implementing a Zero Trust strategy and eliminating your VPN. In a business environment where network expansion is a reality, enabling remote work is necessary, and security breaches have far-reaching consequences, it is past time to move to the Zero Trust security model.

To learn more about implementing Zero Trust security with Unisys, visit unisys.com/security.

Unisys can help you implement Zero Trust security quickly and effectively.

unisys

unisys.com

04/23 WRQ-427-1882