TENEO
OPENING MINDS

Zero Trust Network Access: Use Cases

Work From Anywhere

Zero Trust Network Access enables a work-from-anywhere workforce to access only the applications and data they need to be productive and gives IT teams the peace of mind that operations are secure.

One global construction company deployed a Zero Trust Network Access approach to address the security concerns arising from its hybrid workforce.

The company employs hundreds of engineers and consultants who work remotely 50% of the time and are equipped with laptops to enable this. However, without suitable security measures in place, devices were open to risk of being compromised and becoming a conduit for threats to infiltrate the company network.

As the company grew, its management team became aware of the need to ensure strong cybersecurity. Despite rolling out a range of security solutions, there were still weaknesses in the company's global security strategy.

To remedy these security concerns, the company adopted a Zero Trust Network Access approach, and by applying policies to employees, it also enforced a guest Wi-Fi policy to limit the risk of threat propagation.

Transition to SD-WAN

As SD-WAN is adopted, companies must evolve their security from a perimeter-based framework to a Zero Trust-based framework at the edge.

Many organizations that are migrating to Internet-based architectures consider SD-WAN to be the key enabler due to its link control and ability to drive down the financial onus of MPLS ownership.

They may use broadband or wireless networks to augment or complement the MPLS connections, creating a hybrid WAN. But if they already embrace local or branch Internet breakouts, also known as direct Internet access (DIA), that route traffic to the cloud instead of through a data center, it makes sense to employ a security architecture with the same approach.

Expanding User Ecosystem

Third-party contractors, partners, suppliers, remote workers, and even newly acquired users from mergers and acquisitions all benefit, even accelerate, business.

But provisioning access for this varied and fluid ecosystem introduces risk, increases costs, and creates complexity.

Multi-Cloud Environment

Using multiple private, public, and hybrid clouds for corporate applications can reduce costs, enable flexibility, and accelerate digital transformation.

But a multi-cloud reality also creates complexity and a lack of visibility, exposing organizations to risk.

VPN Elimination

Mobile workforces and cloud-based applications are at odds with legacy and appliance-based access solutions.

Traditional VPNs, proxies, and RDPs drive up operational costs, monopolize already-scarce IT resources, provide limited visibility, offer little in the way of insights, and open business to risk.

One global professional services and tax advisory firm was managing multiple VPNs and used HTTPs to enable different access requirements.

They needed to reduce the management overhead required to support a range of access needs while ensuring industry-leading security and a seamless client experience.

By leveraging a Zero Trust Network Access approach, they dramatically reduced the number of VPNs and the time needed to manage and ensure user access to key company applications.

Find out more

www.teneo.net
info@teneo
UK: +44 118 983 8600
US: +1 703 212 3220