Since the Dot com era, enterprises have relied on network-centric methods to connect users to the network, and by extension the applications running on it. But the way users work has changed, and with applications moving to cloud, the perimeter has extended to the internet. This renders network-centric solutions, like remote access VPNs, which is now obsolete.

The security perimeter now goes beyond the corporate network to include any location where users connect, and applications run. Traditional network security architectures, which are anchored in the data centre and rely on appliances, have become less relevant for modern workflows. These architectures were never designed to scale like a cloud service and were not created for the cloud or mobile environment. Excessive trust makes network-based architectures susceptible as well.
Private apps that were previously only available in the data centre are now being moved to public clouds. Simultaneously, they’re looking for ways to boost productivity by allowing consumers to work from anywhere and on any device. Finding the correct combination of security and user experience is the first step toward success.

Key Challenges in providing a secure Access to Private Applications:

- Placing users on-net, which increases risk
- Providing a poor end-user experience with multiple logins, access controls
- Inbound connections creating opportunity for DDoS attacks
- Requiring appliances, ACLs, and firewall policies
- Lack of ability to provide application segmentation
- Lack of visibility into app-related activity

On-premises network users can migrate laterally across the network. This underlying trust eventually leads to risk and privileged network access. Instead of focusing on a static network border, the security paradigm needs to adapt to focus on the entity, resource, and user device.

Gartner suggests that enterprises use a zero-trust network access service (ZTNA) to safeguard access to private applications because of this shift in focus. Zero-trust network access redefines private application access. There is a need for a cloud service that employs a distributed architecture to provide secure access to data.

Zero-trust network access (ZTNA) is a product or service that provides a logical access boundary around an application or set of applications based on identity and context. The applications are hidden from discovery, and access is limited to a group of identified entities via a trust broker. Before enabling access, the broker verifies the identity, context, and policy adherence of the designated participants and prevents lateral movement elsewhere in the network. This hides application assets from public view and minimizes the attack surface area dramatically. Zero-trust network access (ZTNA) is a product or service that provides a logical access boundary around an application or set of applications based on identity and context. The applications are kept concealed from prying eyes, and access is controlled through a trust broker.

72% of organizations are concerned that VPN may jeopardize IT’s ability to keep their environments secure.

67% of enterprises are considering a remote access alternative to a traditional VPN.

Today, 72% of companies are prioritizing the adoption of a zero trust model.

Remote users connecting through VPN from an approved list of IP addresses are deemed to be trustworthy and are permitted network access through a firewall, which is frequently exposed to the internet.
Zero Trust service works based on four main principles:

- **Context-based**
  Application access should be context-based and not necessitate network connection.

- **Inside-out connections**
  To make apps invisible to unauthorized users, inside-out connections should be employed.

- **App Segmentation**
  Application segmentation should bind users to a single app and prevent them from moving around.

- **Internet**
  The internet must become the new transportation network for businesses.

**How does a Potential Solution for Zero Trust Network Access should Look like:-**

- Mechanism to seek access when a user (employee, third party contractor, or customer) seeks to access an application, there should be controls when the user device verifies the user’s identity and device posture to be verified.

- Creation of application segmentation to avoid unnecessary access to the applications a user may not need to access.

- There should be Controls to check the policy to find the location of the closest application instance to reduce network traffic within the network.

- Use of the client’s location to determine the closest application to the user.

- Securing Connection of two outbound tunnels, one from the device’s and the other from the App.

- The process to happen in real time and automatically.

- Ability to host the solution which can be hosted on-premises or in the cloud.
Coforge is a global digital services and solutions provider, that leverages emerging technologies and deep domain expertise to deliver real-world business impact for its clients. A focus on very select industries, a detailed understanding of the underlying processes of those industries and partnerships with leading platforms provides us a distinct perspective. Coforge leads with its product engineering approach and leverages Cloud, Data, Integration and Automation technologies to transform client businesses into intelligent, high growth enterprises. Coforge’s proprietary platforms power critical business processes across its core verticals. The firm has a presence in 21 countries with 25 delivery centers across nine countries.

Learn more about Coforge at: www.coforge.com