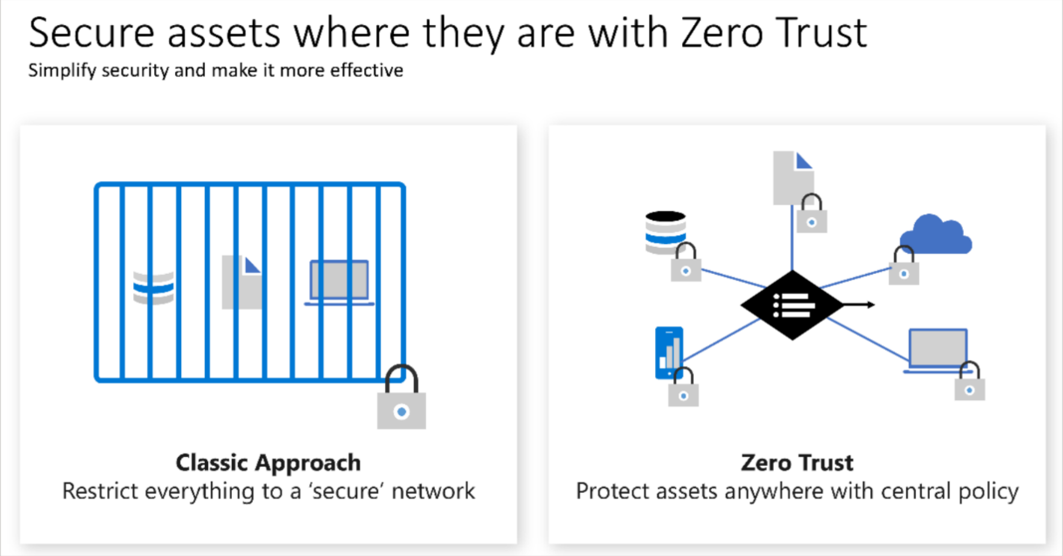
Explore advanced security concepts like zero trust architecture and continuous security monitoring.

Ebuka Obiakor – 20th March 2024



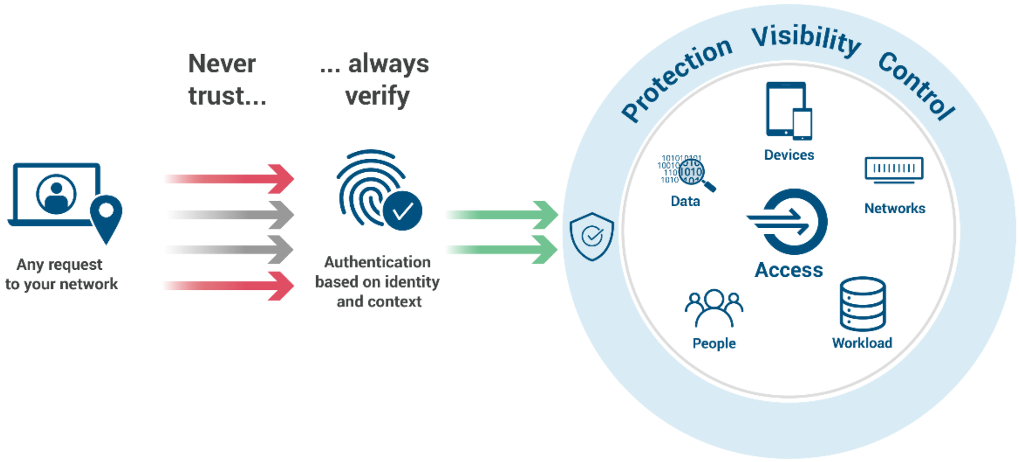
Secure assets where they are with Zero Trust

Simplify security and make it more effective

Classic Approach
Restrict everything to a 'secure' network

Zero Trust
Protect assets anywhere with central policy

Zero Trust Security



Gen-AI assisted

Zero Trust Architecture (ZTA) is a security model based on the principle of "never trust, always verify." It requires all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data.

In a traditional security model, once users and devices are inside a network perimeter, they are often granted access to resources with minimal restrictions. However, with the increasing complexity of modern IT environments and the proliferation of cloud services and mobile devices, traditional perimeter-based security approaches have become less effective in protecting against cyber threats.

Zero Trust Architecture, on the other hand, assumes that threats can exist both inside and outside the network perimeter. Therefore, it advocates for a more granular and dynamic approach to security that verifies the identity of users and devices and applies access controls based on various contextual factors, regardless of their location (inside or outside the network).

Key principles of Zero Trust Architecture include:

1. **Verify Every User:** Rather than assuming trust based on network location or IP address, Zero Trust requires authentication and authorization for every user and device trying to access resources.

2. **Limit Access:** Zero Trust limits access to the minimum required level necessary to perform a specific task. Access is granted based on a variety of factors, including user identity, device health, location, and the sensitivity of the resource being accessed.

3. **Least Privilege:** Users and devices are granted only the permissions necessary to perform their job functions, and access is regularly reviewed and adjusted as needed.

4. **Micro-segmentation:** Zero Trust divides the network into smaller, more manageable segments and applies access controls between each segment. This limits the lateral movement of threats within the network.

5. **Continuous Monitoring:** Zero Trust continuously monitors user and device behavior, network traffic, and other contextual factors to detect and respond to anomalies and potential security threats in real-time.

By implementing Zero Trust Architecture, organizations can improve their security posture by reducing the attack surface, minimizing the risk of data breaches, and enhancing visibility and control over network traffic and user activities. It helps organizations adapt to the changing threat landscape and the increasing complexity of modern IT environments, including cloud computing, mobile devices, and remote work.