Problem Statement

Apex Global Industries is a large, globally distributed enterprise undergoing a multi-year digital modernization initiative. The organization is transitioning its workforce, applications, and collaboration platforms to cloud-based services while migrating legacy on-premises applications to a centralized cloud identity and access model.

This transformation significantly increases the organization's attack surface across identities, endpoints, SaaS applications, cloud workloads, and operational technology environments. Users are no longer confined to a trusted network, applications are no longer hosted in a single environment, and sensitive data is accessed from multiple locations and devices.

The organization currently lacks a unified security architecture that provides consistent access control, visibility, and threat response across cloud and on-premises environments. Traditional perimeter-based security models are insufficient in this context, particularly given the rise of identity-driven attacks, remote access patterns, and lateral movement techniques.

At the same time, Apex Global Industries must meet strict regulatory and compliance obligations, including data residency and privacy requirements, while supporting business objectives such as cost efficiency, simplified collaboration, and improved workforce experience. Security controls must therefore be scalable, cloud-first, and measurable, without introducing excessive friction or disrupting business operations.

In addition, the organization operates operational technology environments that require high availability and limited tolerance for aggressive security enforcement. These environments must be protected through visibility, segmentation, and containment rather than traditional endpoint or network controls.

The core challenge is to define and implement a Zero Trust–aligned security strategy that eliminates implicit trust, enforces continuous verification, and limits blast radius across all assets, while enabling secure remote access, centralized visibility, and rapid incident response at enterprise scale.

This strategy must be technically feasible in a hybrid environment, operationally sustainable over a five-year horizon, and demonstrably effective in reducing security risk while supporting business transformation.