

Zero Trust Architecture for Global Bank

Architecture-first zero trust rollout patterns, identity choke points, and integration with existing SIEM and IAM.

Situation

A large financial institution needed to reduce implicit trust across endpoints and cloud while preserving operational continuity. The goal was defensible segmentation, strong identity signals, and telemetry that security operations could act on.

Approach

We framed trust boundaries, mapped control dependencies, and defined POC exit criteria for identity, device posture, and network enforcement before vendor selection accelerated. Shortlists were weighted on integration cost and operational ownership, not feature lists alone.

Outcomes

Reduced duplicate tooling spend, faster time-to-contain for common incidents, and clearer ownership between IAM, network, and SOC teams.

Use this artifact in stakeholder reviews and procurement discussions.

Contact: contact@cybernexusai.com