OPTIV’S ZERO TRUST CORE PRINCIPLES

EMERGENCE OF ZERO TRUST

The evolution of the trusted perimeter around critical business resources.

OPTIV’S ZERO TRUST JOURNEY

Leveraging understanding and expertise across security domains, Optiv has developed four components that can guide the implementation and optimization of Zero Trust capabilities.

- Design and implement micro-perimeters
- Design dynamic and adaptive perimeters
- Contextualize access and runtime
- Create enhanced security environments

The Zero Trust architecture is a journey that many organizations, while developing security programs, have already embarked on. The below programs, have already embarked on. The below identified gaps by executing periodic assessments to determine remediate the identified gaps by executing periodic assessments, remediate the

THE ZERO TRUST MATURITY JOURNEY

A holistic strategy around cloud access security and governance encompasses four key elements that enable organizations in the management of access specific risks across their cloud infrastructure.

1. Establish a Secure Identity-Based Access Control Environment
2. Assess and Recommend
3. Remediate and Build
4. Transform and Scale

WANT TO LEARN MORE?

Click here to check out the on-demand event hub

OPTIV’S APPROACH TO THE ZERO TRUST JOURNEY

A holistic strategy around cloud access security and governance encompasses four key elements that enable organizations in the management of access specific risks across their cloud infrastructure.

1. Establish a Secure Identity-Based Access Control Environment
2. Assess and Recommend
3. Remediate and Build
4. Transform and Scale

JERRY CHAPMAN

Engineering Fellow, Optiv