Zero Trust Readiness Assessment
Your Zero Trust Journey Starts Here

Expansion of the traditional workforce, ubiquity of security threats and an accelerated digital transformation journey have resulted in a paradigm shift, forever changing the traditional view of ‘trusted network,’ giving rise to the concept of zero trust architecture, which is rooted in the concept of “never trust, always verify.” This architecture relies on an identity and data-centric approach to building dynamic and fluid perimeters around critical assets such as data, applications and networks.

Optiv’s Approach to the Zero Trust Journey

Zero trust can be a confusing concept for many organizations, especially for those that are at an early stage of its adoption. Zero trust is a unified concept, and adopting, building and enhancing a zero trust-based security model requires a broad vision and a practical plan to realize that vision. Optiv’s zero trust security approach aims at taking organizations through a maturity journey that involves establishment and enhancement of capabilities across key security domains.

This journey starts with Optiv’s Zero Trust Readiness Assessment, which helps clients develop and execute on that plan. Optiv’s approach to conducting a Zero Trust Readiness Assessment leverages a framework that amalgamates Optiv’s zero trust principles as well as a capability and maturity framework applied across key security domains. The subsequent outcome of a typical Optiv assessment is a practical roadmap for organizations to build and mature their zero trust capabilities.

Zero Trust Core Principles

1. Establish a Micro Perimeter
2. Establish a Secure, Identity-Based Context to the Resource
3. Create Enhanced Security
4. Continuous Review of Identity and Secure Connection

**ASSESS AND RECOMMEND**
Conduct baseline, and subsequent periodic assessments to determine organizational posture against the zero trust requirements across domains.

**REMEDIATE AND BUILD**
Based on the current state assessments, remediate the identified gaps by executing on a maturity roadmap.

**OPERATE AND OPTIMIZE**
Operate and continue to enhance the zero trust capabilities across the key security domains.
How We Do It

With Optiv’s Zero Trust Assessment, your organization will gain the confidence to plan, build and deploy a successful zero trust architecture utilizing the following steps:

DISCOVER:
- Collaborate with organizational leadership to identify current state capabilities across key security domains
- Collect and organize the acquired information into Optiv’s readiness assessment framework

ANALYZE:
- Leverage the assessment framework to perform a detailed analysis of the acquired information
- Based on the outcome of this analysis, determine organizational capabilities and zero trust readiness across the key domains

RECOMMEND:
- Based on the current and target states, provide a set of recommendations to enhance an organization’s zero trust capabilities
- Develop a time-based prioritized roadmap to enable an organization’s zero trust maturity journey

Case Study

CUSTOMER PROFILE:
Oil and Gas

CLIENT CHALLENGES:
Optiv’s client was looking to address several access and security challenges, including:
- The need for a remote access solution
- Reducing VPN access and authorizing access to specific business assets in the organization
- Moving business critical applications to a micro-segmented network
- Providing enhanced security to critical applications

CLIENT BENEFITS:
- Internal and external access provided through a single solution
- Reduced reliance on VPN for specific set of users and access
- Successful proof-of-concept demonstration to roll out zero trust

OPTIV’S SOLUTION:
Leveraging the lifecycle solution approach, Optiv conducted a Zero Trust Assessment and carried out the following steps:
1. Reviewed and familiarized with the existing VPN and application ingress and egress points defined by the organization
2. Defined policies for external and internal access to critical applications
3. Deployed zero trust solution to support both internal and external access with multi-factor authentication (MFA) integration
4. Provided advisory services for further integration of zero trust elements/capability throughout the organization

The Optiv Advantage

SOLUTION EXPERTISE
- Proactive, outcome-based, risk-driven solutions
- Cross-practice integration

INDUSTRY EXPERTISE
- Zero trust knowledge and thought leadership
- High level of services breadth and depth

INTEGRATED SOLUTIONS
- Immersed into our clients’ unique environments
- Integrated solutions across Optiv’s established and expansive zero trust partnerships

15+ YEARS
- Average experience of Optiv’s Cyber Protection and Identity team with measurable success

CERTIFIED PROFESSIONALS
- CISSP, CISM, CISA, CRISC, CGEIT, CBCP, PMP and ZeroTrust Strategist

Secure your security.”

Optiv is a security solutions integrator – a “one-stop” trusted partner with a singular focus on cybersecurity. Our end-to-end cybersecurity capabilities span risk management and transformation, cyber digital transformation, threat management, cyber operations, identity and data management, and integration and innovation, helping organizations realize stronger, simpler and more cost-efficient cybersecurity programs that support business requirements and outcomes. At Optiv, we are leading a completely new approach to cybersecurity that enables clients to innovate their consumption models, integrate infrastructure and technology to maximize value, achieve measurable outcomes, and realize complete solutions and business alignment. For more information about Optiv, please visit us at www.optiv.com.

©2021 Optiv Security Inc. All Rights Reserved. Optiv is a registered trademark of Optiv Inc.