interlink® energize

interlink® CLOUD ADVISORS

# ZERO TRUST SECURITY WORKSHOP

A workshop that utilizes Zero Trust principles to save your organization both time and money by efficiently reducing risk from attacks and breaches.

## Secure access for your workforce, workloads, and workplace

Reduce risk through an IT Infrastructure Modernization strategy based on the Zero Trust principle of "never trust, always verify." Malicious actors and threats are more advanced than ever, thus Zero Trust no longer assumes your organization is secure based on a firewall or security solutions. This philosophy has data restricted until verification of the right user occurs.

## WORKSHOP OBJECTIVES

### Improve Security

Increase overall visibility into security events, enhance incident response capabilities, and update security policies. This will improve your security posture by reducing risk for your environment.

### Leverage Best Practices

Take advantage of Microsoft's and Interlink's combined security best practices. We see numerous environments from all industries — and know how to best help your organization's security posture in a time-efficient and strategic manner.

### Roadmap

Receive a roadmap deliverable with a prioritized list of action items, deployments, and knowledge transfer sessions to fit within your organization's budget, IT staff capacity to operationalize new security features.

Microsoft Solutions Partner — Modern Work — Specialist: Adoption and Change Management; Calling for Microsoft Teams; Meetings and Meeting Rooms for Microsoft Teams; Teamwork Deployment

Microsoft Solutions Partner — Security — Specialist: Identity and Access Management; Threat Protection; Information Protection and Governance

Microsoft Solutions Partner — Infrastructure; Azure — Specialist: Infra and Database Migration; Microsoft Windows Virtual Desktop

Microsoft Solutions Partner — Digital & App Innovation; Azure

interlink® CLOUD ADVISORS

www.interlink.com | hello@interlink.com | 800-900-1150

# ZERO TRUST PRINCIPLES

This modern security strategy reconciles today's complex environment and mobile workforce. Zero Trust helps you by continuously protecting and verifying people, devices, and data wherever they are located. Traditionally, approaches that attempt to force all assets onto a "secure and compliant" network fall short if identity theft occurs. Zero Trust mitigates this by focusing on the security and compliance of assets regardless of their physical or network location. Zero Trust teaches the importance of "never trust, always verify."

## Verify Explicitly

Reduce risk by authenticating users and authorizing access based on identity, location, device health, service or workload, and classification of data.

## Use Least Privilege

Limit user access with just-in-time and just-enough-access, risk-based adaptive policies, and data protection to help secure both data and productivity.

## Assume Breach

Minimize breach impact by implementing end-to-end encryption, limit access by policy and network micro-segmentation, and by using enhanced threat detection and response tools for rapid threat isolation.

**CONTACT INTERLINK TODAY TO LEARN MORE ABOUT THIS WORKSHOP AND DISCUSS YOUR SPECIFIC ENVIRONMENT!**

Microsoft Solutions Partner — Modern Work — Specialist: Adoption and Change Management; Calling for Microsoft Teams; Meetings and Meeting Rooms for Microsoft Teams; Teamwork Deployment

Microsoft Solutions Partner — Security — Specialist: Identity and Access Management; Threat Protection; Information Protection and Governance

Microsoft Solutions Partner — Infrastructure, Azure — Specialist: Infra and Database Migration; Microsoft Windows Virtual Desktop

Microsoft Solutions Partner — Digital & App Innovation, Azure

interlink® CLOUD ADVISORS

www.interlink.com | hello@interlink.com | 800-900-1150

# WITH A ZERO TRUST STRATEGY, INTERLINK WILL ASSESS THE FOLLOWING TO REDUCE RISK AND IMPROVE SECURITY:

## Identity

Leverage Microsoft Azure Active Directory to optimize your user sign-in experience and increase assurance that connections to corporate apps and data are from trusted users and devices.

## Endpoints

Leverage Microsoft Endpoint Manager to assess your organization's endpoint management approach to define, deploy, and enforce policies that secure data, and verify device/application health and security.

## Networks

Follow Azure Security Center best practices to secure Azure Networking and evaluate if your organization can leverage the Azure Global WAN and Azure services to provide secure and affordable remote access solutions.

## Applications

Leverage Microsoft Cloud App Security to gain visibility into SaaS cloud apps use, classify apps in use as sanctioned or unsanctioned, and then deploy and enforce information protection, threat protection, and conditional access policies on app access and app session activity.

## Data

Utilize Microsoft Information Protection to classify, label, encrypt and secure the flow of corporate data to Office 365 services and 3rd party SaaS applications.

## Infrastructure

Deploy least privilege access controls, further protect endpoints, use security incident and event data from infrastructure servers and services to detect attacks and anomalies, and automatically flag or block risky behaviors.

## How can Interlink help?

**Contact Interlink Cloud Advisors today to learn more about this engagement and discuss your specific needs!**

Microsoft Solutions Partner
Modern Work
Specialist
Adoption and Change Management
Calling for Microsoft Teams
Meetings and Meeting Rooms for Microsoft Teams
Teamwork Deployment

Microsoft Solutions Partner
Security
Specialist
Identity and Access Management
Threat Protection
Information Protection and Governance

Microsoft Solutions Partner
Infrastructure
Azure
Specialist
Infra and Database Migration
Microsoft Windows Virtual Desktop

Microsoft Solutions Partner
Digital & App Innovation
Azure

interlink® CLOUD ADVISORS

www.interlink.com | hello@interlink.com | 800-900-1150