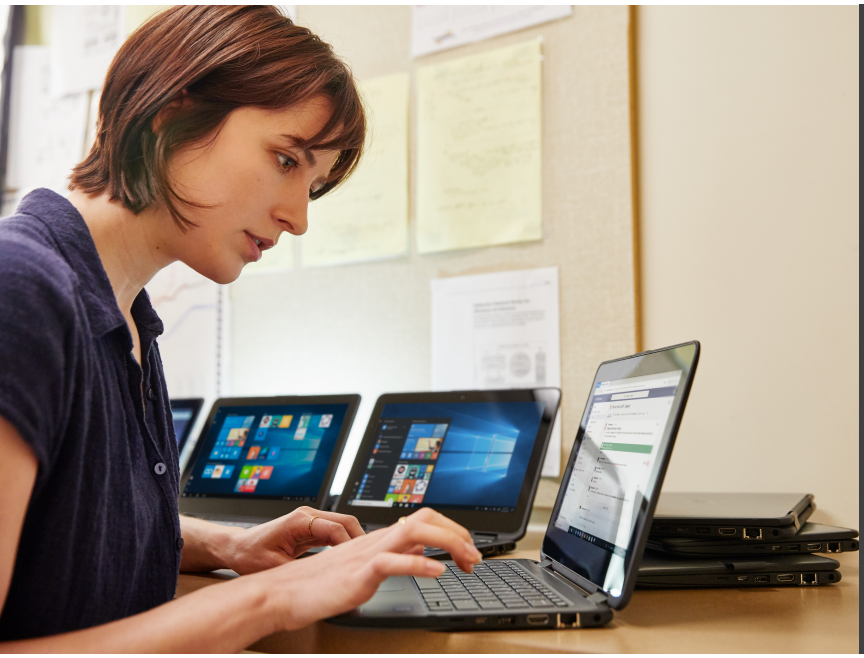

Zero-Trust Secure Email Offering

> Platform Assessment
> Solution Design
> Pilot Implementation

English | Spanish

Email is **the biggest threat vector** in the organization. Malware, insider exfiltration, spam, and sophisticated phishing attacks are rising rapidly. In fact, more than 90% of phishing attacks are carried out through email.

Our secure email solution is based on the latest trend in security: the **Zero Trust Framework**. It focuses on how users engage with technology to improve their security maturity level, an essential protection against social engineering attacks.

Execution plan:

Envision

- Validate your vision, use cases, and business requirements
- Strategic review of your existing platform

Plan

- Define the functional solution requirements
- Design a customized solution architecture, according to your needs
- Detailed project plan

Deploy

- Implement the solution in your production environment to a limited scope of users
- End user training and solution empowerment
- Actionable findings, recommendations, and next steps

Scope included in the workload:

Identity - Advanced Identity Protection leveraging Azure AD Conditional Access [up to 3 uses cases]

Applications – App Protection Policies for mobiles device [MAM]

Threat Protection – Advanced Threat Protection leveraging Microsoft Defender for Office [Up to 3 use cases]

Why Zero Trust?

- **Always assume breach**
  The Zero Trust model assumes breach and verifies each request as though it originates from an open network.
- **Explicitly verify**
  Fully authenticate, authorize, and encrypt every access request before granting access.
- **Apply least privileged access**
  Minimize lateral movement through micro-segmentation and principle of least privilege.
- **Real-time response**
  Detect and respond to anomalies in real time, using rich intelligence and analytics.

Up to 3 of the below technological controls
(recommendations in **bold**)

Identity

- **Conditional access**
- Secure external collaboration

Devices

- Enforce and manage device policies
- Protect applications
- Conditional access
- Security compliance
- Platform

Applications

- Azure AD/SPO/OD4B/Teams services hardening
- Access controls based on application restrictions
- **Application protection**
- Conditional access

Data

- Data protection
- Confidentiality-based access controls
- Tagging-based session controls
- Discovery and response

Threat Protection

- **Threat detection & protection**
- Risk-based protection

Analysis, Monitoring, and Alerts

- Platform analytics and monitoring
- E-Visor for M365 / Teams

Additional technological controls available as add-on

Time:
- Up to six business weeks

Price:

$75K

SYNERGY ADVISORS

Contact us: solutions@synergyadvisors.biz