Information Technology of Egypt Corporation - ITE Corp

Microsoft Zero Trust Assessment (ZTA)

Plan your end-to-end security architecture with a Zero Trust approach

SECURITY MODERNIZATION WITH ZERO TRUST PRINCIPLES

Business Enablement

Align security to the organization's mission, priorities, risks, and processes

Assume Breach (Assume Compromise)

Assume attackers can and will successfully attack anything (identity, network, device, app, infrastructure, etc.) and plan accordingly

Verify Explicitly

Protect assets against attacker control by explicitly validating that all trust and security decisions use all relevant available information and telemetry.

Use least privilege access

Limit access of a potentially compromised asset, typically with just-in-time and just-enough-access (JIT/JEA) and risk-based polices like adaptive access control.

ZERO TRUST ARCHITECTURE

Access and Identity

Data Security

IoT and OT Security

Modern Security Operations (SecOps/SOC)

Infrastructure & Development Security

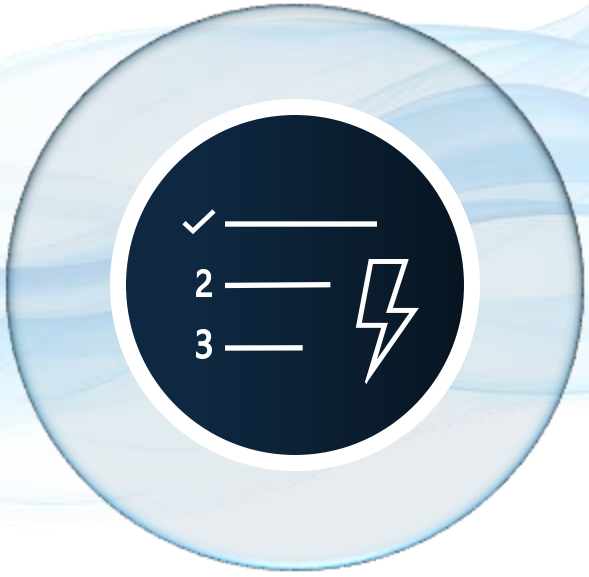
ZERO TRUST ASSESSMENT
PILLARS

PILLAR ONE
IDENTITY

Verify every user, service account, and identity with strong authentication mechanisms And Assessment focuses on identity lifecycle management, least privilege enforcement

MFA

User-friendly Multifactor Authentication



Conditional Access

Configurable Conditional Access policies based on context and risk assessment

Behavior Analytics

User and entity behavior analytics to automatically protect against identity compromise

PILLAR TWO
ENDPOINTS

Continuously evaluate device health, compliance status, and security configuration posture. Assessment covers endpoint detection and response (EDR) capabilities Every connected endpoint must meet security baselines before gaining access to resources.

Device Health

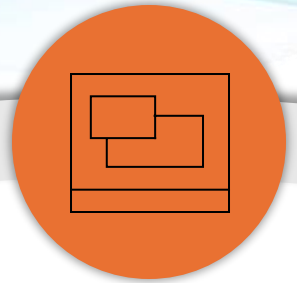
- Real-Time Monitoring of patches
- Antivirus status
- Security Stack configuration
- OS and security baseline

EDR Capabilities

Advanced threat detection and automated response across all endpoints

Compliance Posture

Continuous verification against organizational security policies and standards



PILLAR THREE
APPLICATIONS

Maintain complete visibility and control over all applications and APIs operating across your environment: on-premises legacy systems, cloud-native applications, SaaS platforms, and custom-developed solutions.

Assessment includes access control evaluation, shadow IT discovery to identify unauthorized applications, in-application permission management, and behavioral analytics for detecting compromised accounts and malicious activity within applications and workloads.

App Inventory

Discover and catalog all applications and APIs across your infrastructure

Access Controls

Enforce identity-based access policies and permission boundaries

Threat Detection

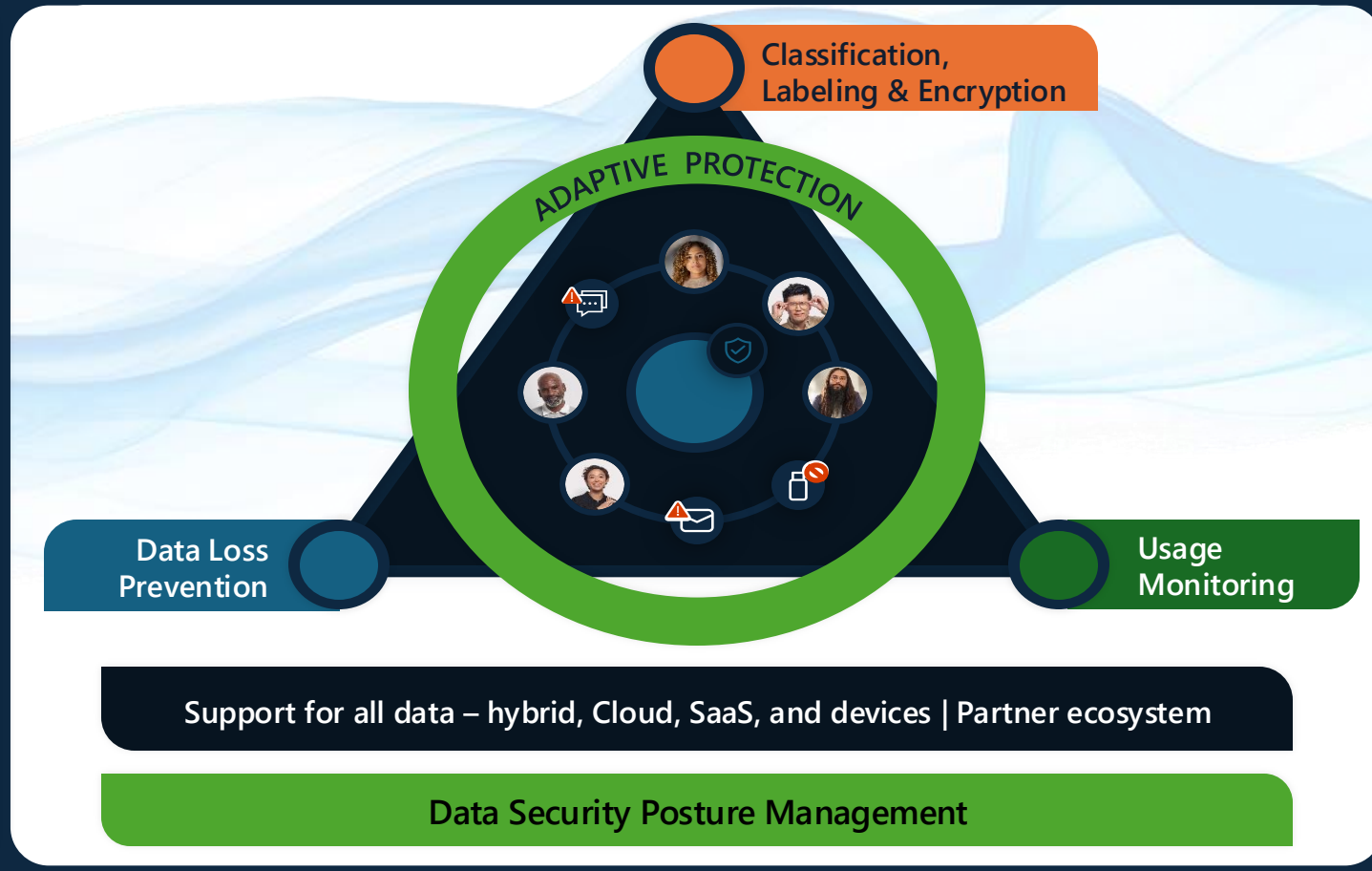
Enable real-time behavior analytics and and anomaly detection within applications

PILLAR FOUR
DATA

Protect sensitive information through **classification**, **labeling**, and encryption wherever data resides or travels. Assessment evaluates data access policies

extends beyond organizational boundaries into cloud storage, third-party applications, and mobile devices.

Enable **Adaptive Protection** to assign high-risk users to appropriate DLP, Data Lifecycle Management.



PILLAR FIVE
INFRASTRUCTURE

Assess the security posture of all infrastructure components including servers, virtual machines, containers, microservices—both on-premises and cloud-hosted.
Evaluate configuration management practices, implement just-in-time (JIT) access for administrative privileges, and deploy comprehensive telemetry for anomaly detection.
Harden infrastructure to reduce the attack surface and enable automated threat response when suspicious activity is detected.

Configuration Management

Enforce baseline security configurations across all infrastructure

Just-In-Time Access

Minimize standing privileges with time-limited administrative access

Telemetry & Monitoring

Collect comprehensive logs and performance data for threat detection

PILLAR SIX
NETWORK

Implement network segmentation and micro-segmentation to limit lateral movement and contain potential threats.
Assessment covers encryption protocols, real-time threat protection capabilities, network monitoring depth, and advanced analytics.
Enhanced network visibility enables rapid detection and blocking of suspicious activities, preventing attackers from moving freely across your network even if they breach an initial entry point.

Network Segmentation
Divide networks into secure zones to limit attacker movement and isolate sensitive systems

Encryption
Encrypt all network traffic to protect data in transit and prevent eavesdropping

Threat Protection
Deploy advanced threat detection and automatic blocking of malicious network traffic

ZERO TRUST ASSESSMENT
PHASES AND ACTIVITIES

PRE-ENGAGEMENT CALL

- Introductions
- Engagement walk-through
- Expectations
- What's next

ENGAGEMENT SETUP & SCOPE DEFINITION MEETING

- Overview of the engagement products
- Engagement scope and design decisions

ENGAGEMENT

- Go through Zero Trust assessment
- Go through the Secure score portal

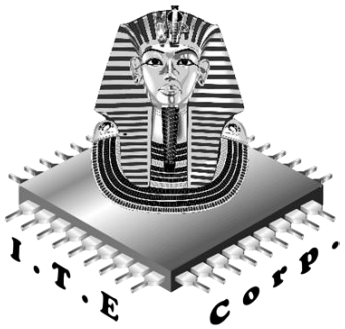
ZERO TRUST ASSESSMENT
PHASES AND ACTIVITIES

RESULTS PRESENTATION

- Results presentation and Next Steps discussion.

PREPARING FOR IMPLEMENTATION OR DEMO

- Prepare Demo
- Prepare Implementation



THANK YOU