peopleXTECH

A **Quest Global**Company

ZERO TRUST OPTIMIZATION AGENT

USA : +1 206-858-9902
INDIA : +91 40 41239999

18300 NE Union Hill Road
Suite 210 Redmond, WA 98052

Info@peopletech.com
www.peopletech.com

Table of Contents

01 Purpose of the Agent 3

02 Functional Design 3

03 Triggers for Agent Activation 3

04 Plugins or Data Signals 4

05 Customer Onboarding / Deployment 4

01 Purpose of the Agent

The Zero-Trust Posture Optimization Agent acts as a virtual security architect, automatically and continuously evaluating your cloud environment against Zero-Trust principles.

Instead of waiting for an attack, this agent proactively hunts for misconfigurations, compliance drift, and security gaps that attackers love to find. It correlates data from across your environment to give you a single, prioritized list of what to fix first.

Associated Microsoft Products:
- Microsoft Entra ID

02 Functional Design

Our agent will:
- Query posture: Run KQL queries against Microsoft Sentinel to retrieve Secure Score changes and top failing controls.
- Query devices: Identify noncompliant devices from Intune logs and map them to users and roles.
- Query identity: Identify Conditional Access gaps such as unmanaged devices, legacy authentication, and missing MFA.
- Correlate risks: Link identity, device, and cloud posture risks to highlight high-priority issues (e.g., privileged users on noncompliant devices).
- Produce recommendations: Generate a prioritized list of remediation steps with estimated risk reduction.
- Report: Deliver results in a Markdown/HTML report, optional JSON payload for ticketing, and optional Teams post.

03 Triggers for Agent Activation

The agent can run in two modes:

Scheduled scan: Runs daily at 02:00 UTC.

Event-driven scan: Runs immediately when any of the following occur:
- A new Conditional Access policy is created.
- A new noncompliant device is detected.
- The Secure Score drops by more than 5 points in 24 hours.

04 Plugins or Data Signals

Required Data Signals via Microsoft Sentinel:

- Microsoft Entra ID: Conditional Access policies and sign-in logs.

Required Permissions:

- Microsoft Sentinel Log Analytics Reader access to the workspace.

05 Customer Onboarding / Deployment

Preconditions:

- Customer must have an active Microsoft Sentinel workspace.
- The Microsoft Entra ID data connector must be enabled.
- The agent must be granted read/query access to the Sentinel workspace.

Deployment Steps:

1. Install the agent from the Security Copilot Agents gallery.
2. Configure tenant and workspace details.
3. Assign Log Analytics Reader role to the agent identity.
4. Validate that all required data connectors are active.