peopleXTECH

A **Quest Global**Company

Shadow SaaS Discovery 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

1. Purpose of the Agent

The **Shadow SaaS Discovery Agent** helps organizations detect and control unauthorized SaaS applications that employees use without IT approval (Shadow IT). It finds unsanctioned apps, identifies who uses them, checks their risk level, and provides remediation advice (for example, revoke access or approve safely). This enables security teams to reduce data leakage risks, improve compliance, and maintain visibility of all applications connected to Microsoft 365 accounts.

The agent detects unauthorized SaaS applications within an enterprise environment. It monitors user sign-ins, OAuth consents, endpoint network activity, and Microsoft 365 operations to identify unsanctioned applications and assess associated risk. The agent produces a consolidated report of discovered SaaS applications, related users, and recommended actions.

Associated Microsoft Products:

- Microsoft Sentinel
- Microsoft Entra ID
- Microsoft Defender for Endpoint
- Microsoft 365

2. Functional Design

- Collect SigninLogs from Microsoft Entra ID to identify access to external SaaS platforms.
- Analyze AuditLogs to detect new or modified OAuth consents granted to third-party applications.
- Use DeviceNetworkEvents from Microsoft Defender for Endpoint to detect network connections to SaaS domains.
- Examine logs from Microsoft 365 to correlate file uploads or sharing with detected SaaS applications.
- Aggregate detections into a normalized dataset containing user, device, and application details.
- Perform risk scoring using SaaSAnalyzerSkill based on permissions, activity frequency, and exposure level.
- Generate a weekly Shadow SaaS Discovery Report summarizing findings with risk categorization and recommended remediation actions in a structured format (App Name, User, Device, Risk Level, Action).

3. Triggers for Agent Activation

The agent runs automatically in two ways: it performs a scheduled scan every week to check the entire environment, and it also scans based on the last working date to detect any new or changed SaaS activities. Additionally, it runs instantly when certain events occur, such as a new OAuth consent to an external app, a new app or service principal creation in Entra ID, or SaaS-related network activity on managed devices.

4. Plugins or Data Signals

Required Data Sources

1. Microsoft Entra ID – Uses *SigninLogs* and *AuditLogs* to detect user sign-ins and OAuth consents.
2. Microsoft Defender for Endpoint – Uses *DeviceNetworkEvents* to identify SaaS domain access from managed devices.
3. Microsoft 365 – Uses logs to correlate file activity with SaaS usage.

Required Integrations:

1. Microsoft Sentinel data connection.
2. Log Analytics Reader permission for workspace access.
3. Sentinel KQL plugin for cross-source data retrieval.

5. Customer Onboarding / Deployment

Preconditions

- Microsoft Sentinel workspace configured with Log Analytics.
- Data connectors for Entra ID, Defender for Endpoint, and Microsoft 365 enabled.

Deployment Procedure

1. Install the agent from the Security Copilot Agent Gallery.
2. Configure the following parameters:
    - Tenant ID
    - Subscription ID
    - Resource Group Name
    - Workspace Name
3. Assign the Log Analytics Reader role to the agent identity.

4. Confirm operational status of all required data connectors.
5. (Optional) Configure automated remediation via Microsoft Logic Apps.