# AZURE AD

## Cloud Inspector

**WHAT IS THE AZURE AD INSPECTOR?**

This is Liongard's dedicated inspector for Azure Active Directory, Microsoft's cloud-based identity and access management service. Azure Active Directory is used to mediate account logins and policies, and for the management of devices joined to Azure Active Directory and managed by the Intune mobile device management (MDM) platform.

This inspector returns data such as:

- → Azure Active Directory users and groups
- → Intune devices and policies
- → Security information, including risk detections and risky users

**WHY IS IT IMPORTANT?**

Azure Active Directory and other cloud-based directory services are increasingly supplanting on-premise solutions like Active Directory as the primary source of identity and policy management for modern organizations. As the world continues to shift toward remote working, MSPs are having to switch over to cloud directory services to get better insight and manage remote workstations.

By allowing Partners a method for inspecting Azure Active Directory, Liongard provides the visibility necessary to stay on top of the issues that matter most to you and your customers.

**NOTE**

This inspector is most beneficial for MSPs with premium Azure Active Directory subscriptions, and it does not inspect Teams or SharePoints.

## Use Cases

| MSP USER | USE CASE |
|---|---|
| **As an MSP security engineer …** | … I would like to create alerts to notify my team of issues such as logins from unapproved locations, risk detections and risky users, so we can detect possible security breaches. |
| **As an MSP security engineer …** | … I would like central visibility and alerting capability on devices managed by Intune, to determine whether or not they comply with my security policies. |
| **As an MSP engineer managing Apple devices via Intune …** | … I would like to create an alert when VPP tokens are approaching expiration, to prevent disruptions of service to my customers. |

**DETAILS ON DATA GATHERED**

- → Group permissions
- → Users without MFA
- → Intune Policies
- → User sign-ins logs
- → Device Compliance
- → Risky user levels

**ALERTS AVAILABLE**

- → Risky User Identified
- → Application Sign-in Success has dropped
- → App Policies Changed
- → VPP token expiration

liongard