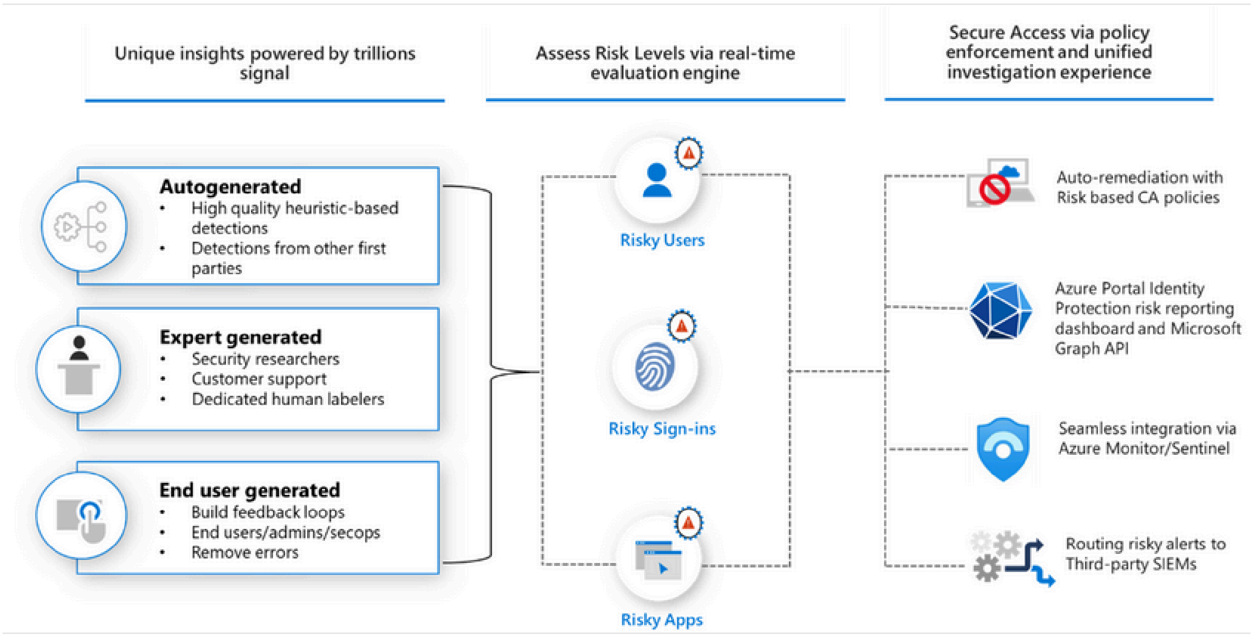
What is Identity Protection?


Unique insights powered by trillions signal
Assess Risk Levels via real-time evaluation engine
Secure Access via policy enforcement and unified investigation experience
Autogenerated
High quality heuristic-based detections
Detections from other first parties
Expert generated
Security researchers
Customer support
Dedicated human labelers
End user generated
Build feedback loops
End users/admins/secops
Remove errors
Risky Users
Risky Sign-ins
Risky Apps
Auto-remediation with Risk based CA policies
Azure Portal Identity Protection risk reporting dashboard and Microsoft Graph API
Seamless integration via Azure Monitor/Sentinel
Routing risky alerts to Third-party SIEMs

Entra is derived from the Latin “intrare”, meaning “**to enter**”. ID is an abbreviation for “identity”. Entra ID signifies **Microsoft's** mission to enable users to enter any application or resource with their identity, regardless of where they are or what device they use.

Microsoft Entra ID (formerly Azure AD) Protection helps organizations detect, investigate, and remediate identity-based risks. These identity-based risks can be further fed into tools like Conditional Access to make access decisions or fed back to a security information and event management (SIEM) tool for further investigation and correlation.

Detect risks

Microsoft continually adds and updates detections in our catalog to protect organizations. These detections come from our learnings based on the analysis of trillions of signals each day from Active Directory, Microsoft Accounts, and in gaming with Xbox. This broad range of signals helps Identity Protection detect risky behaviors like:

- Anonymous IP address usage
- Password spray attacks
- Leaked credentials
- and more...

During each sign-in, Identity Protection runs all real-time sign-in detections generating a sign-in session risk level, indicating how likely the sign-in is compromised. Based on this risk level, policies are then applied to protect the user and the organization.

Investigate

Any risks detected on an identity are tracked with reporting. Identity Protection provides three key reports for administrators to investigate risks and take action:

- **Risk detections:** Each risk detected is reported as a risk detection.
- **Risky sign-ins:** A risky sign-in is reported when there are one or more risk detections reported for that sign-in. Atypical travel, Malware Linked IP, and anonymous IP address.
- **Risky users:** A Risky user is reported when either or both of the following are true:
    - The user has one or more Risky sign-ins.
    - One or more risk detections are reported.

Remediate risks

Why is automation critical in security?

> Analyzed ...**24 trillion security signals** combined with intelligence we track by monitoring more than 40 nation-state groups and over 140 threat groups...
>
> ...From January 2021 through December 2021, we've blocked more than 25.6 billion Microsoft Entra brute force authentication attacks...

The sheer scale of signals and attacks requires some level of automation just to keep up.

Automatic remediation

Risk-based Conditional Access policies can be enabled to require access controls such as providing a strong authentication method, perform **multi factor authentication**, or perform a secure password reset based on the detected risk level. If the user successfully completes the access control, the risk is automatically remediated.

Manual remediation

When user remediation isn't enabled, an administrator must manually review them in the reports in the portal, through the API, or in Microsoft 365 Defender. Administrators can perform manual actions to dismiss, confirm safe, or confirm compromise on the risks.