



Microsoft
CERTIFIED

EXPERT



Detecting and Responding to Identity Risks with Microsoft Entra ID Protection

Combining AI-driven risk signals with Conditional Access for
secure authentication

#PerparimLabs #MicrosoftEntra #IdentityProtection
#ZeroTrust #CloudSecurity

(P) PerparimLabs

What Is Entra ID Protection?



Formerly *Azure AD Identity Protection*



Detects, investigates, and remediates identity-based risks



Uses AI signals like location, device, and behavior



Integrates with Conditional Access and Sentinel for automated defense

How Risk Detection Works



Risky sign-ins: Detected during authentication (e.g., atypical travel, anonymous IPs)



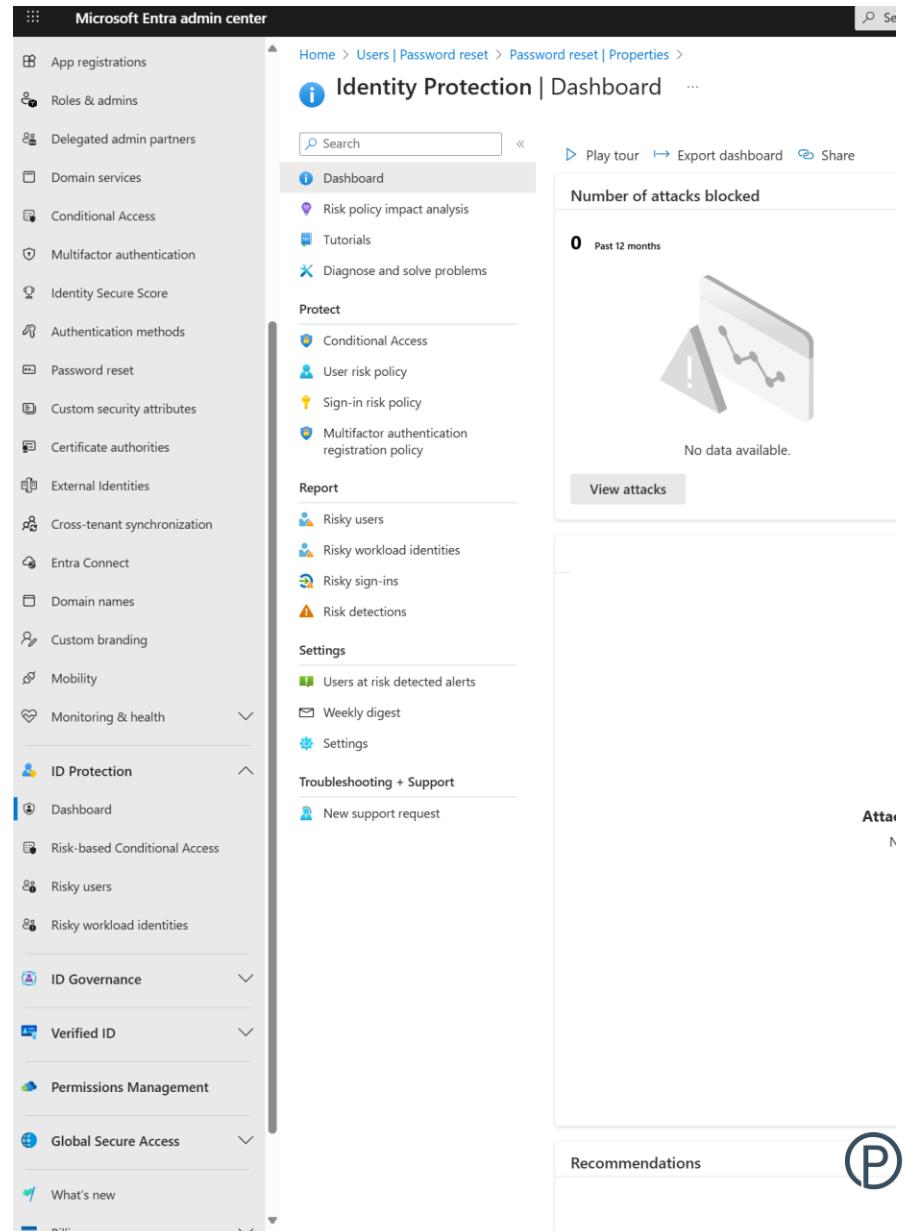
Risky users: Based on behavior anomalies or dark web credential leaks



Microsoft AI analyzes **trillions of signals** to assign risk levels (Low / Medium / High).

Dashboard Overview

- Centralized view of risky users, sign-ins, and policy enforcement.



The screenshot shows the Microsoft Entra admin center with the 'Identity Protection' dashboard selected. The left sidebar contains a navigation menu with sections like App registrations, Roles & admins, Delegated admin partners, Domain services, Conditional Access, Multifactor authentication, Identity Secure Score, Authentication methods, Password reset, Custom security attributes, Certificate authorities, External Identities, Cross-tenant synchronization, Entra Connect, Domain names, Custom branding, Mobility, Monitoring & health, ID Protection, ID Governance, Verified ID, Permissions Management, Global Secure Access, and What's new. The main content area displays a summary of 'Number of attacks blocked' (0 for the past 12 months) with a chart showing a line with a downward trend. It also includes sections for Protect (Conditional Access, User risk policy, Sign-in risk policy, Multifactor authentication registration policy), Report (Risky users, Risky workload identities, Risky sign-ins, Risk detections), Settings (Users at risk detected alerts, Weekly digest, Settings), and Troubleshooting + Support (New support request). A 'View attacks' button is present. At the bottom, there is a 'Recommendations' section and the PerparimLabs logo.

#PerparimLabs #MicrosoftEntra #IdentityProtection
#ZeroTrust #CloudSecurity



Sign-in Risk Policy

- Applied to all users
- Risk threshold: *Medium and above*
- Action: *Require MFA*
- Reinforces Zero Trust by verifying user authenticity before access.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar contains a navigation menu with various options like App registrations, Roles & admins, and Conditional Access. The main content area is titled "Identity Protection | Sign-in risk policy". It includes a search bar, a message about migrating to Conditional Access, and sections for "Policy Name" (set to "Sign-in risk remediation policy"), "Assignments" (set to "All users included and 1 user excluded"), and "Sign-in risk" (set to "Medium and above"). The "Protect" section is expanded, showing "Sign-in risk policy" as the selected option. The "Report" section lists Risky users, Risky workload identities, and Risky sign-ins. The "Controls" section shows "Access" (set to "Require multifactor authentication"). The "Settings" section includes "Users at risk detected alerts", "Weekly digest", and "Settings". A "Troubleshooting + Support" section with a "New support request" button is also present. At the bottom, there is a "Policy enforcement" section with "Enabled" and "Disabled" buttons, and a "Save" button.

User Risk Policy

- Triggered when abnormal user activity occurs (odd login times, leaked credentials)
- Action: *Require password change*
- Level: *Low and above* — most sensitive policy

The screenshot shows the Microsoft Entra admin center interface. The left sidebar contains a navigation menu with various options like App registrations, Roles & admins, Delegated admin partners, Domain services, Conditional Access, Multifactor authentication, Identity Secure Score, Authentication methods, Password reset, Custom security attributes, Certificate authorities, External Identities, Cross-tenant synchronization, Entra Connect, Domain names, Custom branding, Mobility, Monitoring & health, ID Protection, Risk-based Conditional Access, Risky users, Risky workload identities, ID Governance, Verified ID, Permissions Management, Global Secure Access, and What's new. The 'Sign-in risk policy' option under 'Protect' is highlighted. The main content area is titled 'Identity Protection | Sign-in risk policy'. It includes a search bar, a note about migrating to Condition, and sections for Policy Name (Sign-in risk remediation policy), Assignments (Users: All users included and 1 user excluded, Sign-in risk: Medium and above), Controls (Access: Require multifactor authentication), and Settings (Users at risk detected alerts, Weekly digest, Settings). A 'Save' button is at the bottom right. A status bar at the bottom indicates 'Policy enforcement: Enabled'.

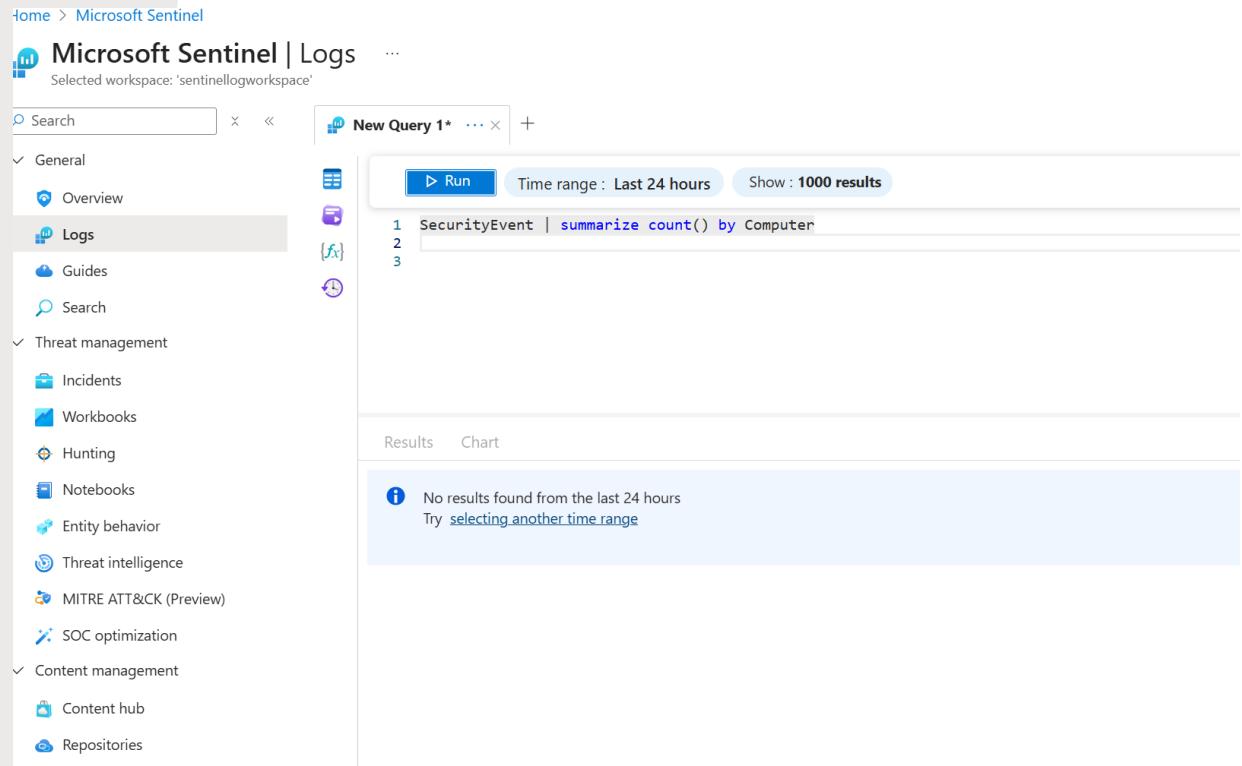
Risky User Monitoring

- In production environments, this report populates automatically with risky sign-ins and behaviors, allowing security teams to take proactive actions.

The screenshot shows the Microsoft Entra admin center interface. The left sidebar contains a navigation menu with categories like Domain services, Conditional Access, Multifactor authentication, Identity Secure Score, Authentication methods, Password reset, Custom security attributes, Certificate authorities, External Identities, Cross-tenant synchronization, Entra Connect, Domain names, Custom branding, Mobility, Monitoring & health, ID Protection, Risk-based Conditional Access, Risky users, Risky workload identities, ID Governance, Verified ID, Permissions Management, Global Secure Access, What's new, Billing, Diagnose & solve problems, and New support request. The main content area is titled 'Identity Protection | Risky users' and displays a search bar, a message about automatic risk remediation, and a table with columns for Learn more, Download, Select all, and checkboxes for 'Confirm user(s) compromised' and 'Confirm user(s) safe'. The table shows 2 selected users in the 'Risk state' column and an 'Active' status. A message at the bottom states 'No risky users found'.

Sentinel Integration

- Logs can be queried from Microsoft Sentinel for risk correlation.
- Even when no live data is found, this lab demonstrates how Entra Identity Protection can feed SIEM pipelines through *Log Analytics workspace integration*.



The screenshot shows the Microsoft Sentinel Logs interface. The left sidebar contains navigation links for General (Overview, Logs, Guides, Search), Threat management (Incidents, Workbooks, Hunting, Notebooks, Entity behavior, Threat intelligence, MITRE ATT&CK (Preview), SOC optimization), and Content management (Content hub, Repositories). The main area shows a query editor with the following content:

```
1 SecurityEvent | summarize count() by Computer
2
3
```

The query results pane indicates "No results found from the last 24 hours. Try selecting another time range".

Key Takeaways

- ✓ Detect risks automatically using AI signals
- ✓ Enforce MFA or password reset based on risk level
- ✓ Integrate with Sentinel for continuous monitoring
- ✓ Simplify remediation with automation and reports

