Oort + Microsoft

Added Identity Protection for Entra ID

Prevent, detect, and respond to identity threats

Active Directory has been a critical source of data for security teams for several years. Now, with more organizations shifting to the cloud, Oort protects identities in Microsoft Entra ID.

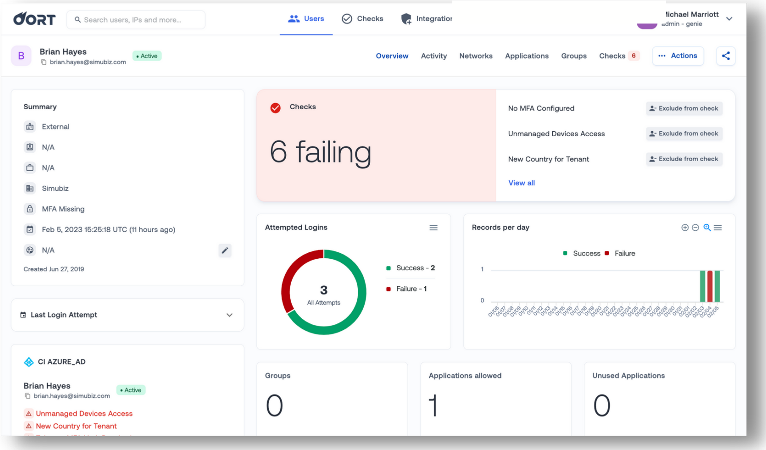
Key Benefits

- **Quickly** triage Microsoft Entra ID risky users alerts
- **Identify** Microsoft Entra ID Admin activity anomalies
- **Detect** unmanaged device access from Intune
- **Cleanup** inactive guest accounts
- **Lock down** service accounts
- **Correlate** data from Entra ID with other identity platforms and applications
- **Consume** insights in Azure Sentinel or other SIEM/Ticketing platforms
- **Create** effective response options in Microsoft Teams and Slack

Quickly triage risky users alerts

Microsoft's Identity Protection (Entra ID Premium P2) provides potential indications of risk, but the high false positive rate often results in them being ignored by security teams. The majority (68.2%) of Microsoft risk events are low-risk. Investigating alerts is difficult in Microsoft Entra ID without more context.

Oort ingests Microsoft risk indicators and correlates them with information from other identity platforms and threat feeds to create its own, low noise detections. Furthermore, with Oort's User 360 profiles, it's quick and easy to investigate the impacted user and assess the true risk.



Brian Hayes
brian.hayes@simubiz.com
• Active

Summary
External
N/A
N/A
Simubiz
MFA Missing
Feb 5, 2023 15:25:18 UTC (11 hours ago)
N/A
Created Jun 27, 2019

Checks
6 failing

No MFA Configured — Exclude from check
Unmanaged Devices Access — Exclude from check
New Country for Tenant — Exclude from check
View all

CI AZURE_AD
Brian Hayes
brian.hayes@simubiz.com
• Active
Unmanaged Devices Access
New Country for Tenant

Groups
0

Applications allowed
1

Unused Applications
0

Identify unmanaged device access

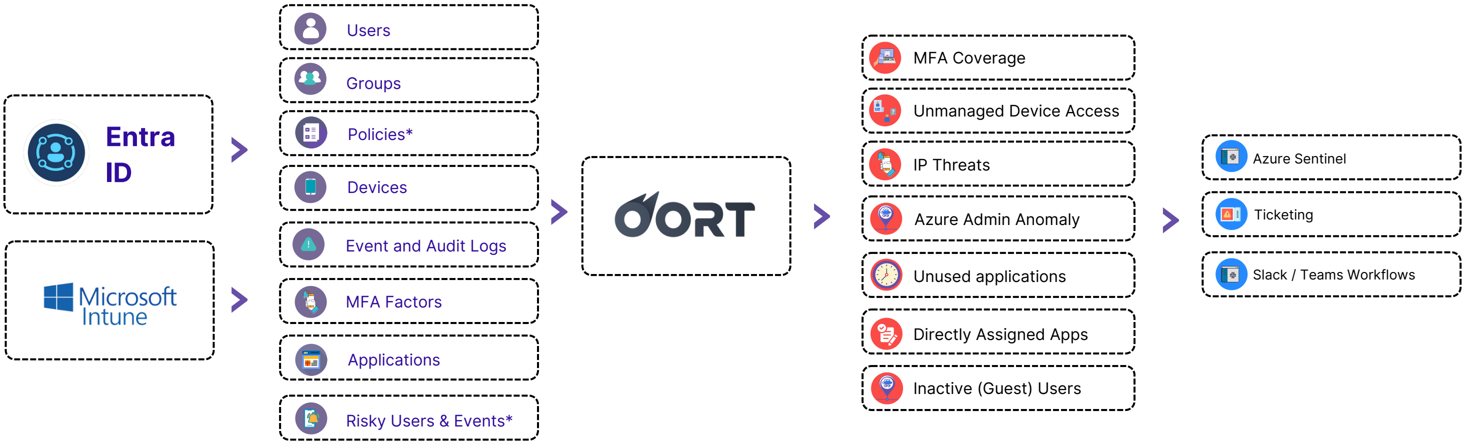
Organizations are turning to device trust to harden their identity attack surface. Oort provides visibility of device data from Intune that you do not get with Entra ID Premium packages. Oort identifies users who are still logging in from unmanaged devices, making it possible to identify and deprecate unmanaged device access when the organization is fully ready.

Clean up unused permissions and inactive accounts

With Oort, teams can easily clean up inactive guest accounts and lock down service accounts - saving organizations on licensing costs while stopping the takeover of dormant accounts.

Oort: A Security Layer On Top Of Azure AD

How it Works



*Available on Microsoft Entra ID Premium P2

Getting Started

Results in 30 Minutes

Oort is extremely fast to work with and customers often get results within their first 30 minutes. This is all achieved without expensive scripting, custom rules, or log management.

Step 1: Add New Integration

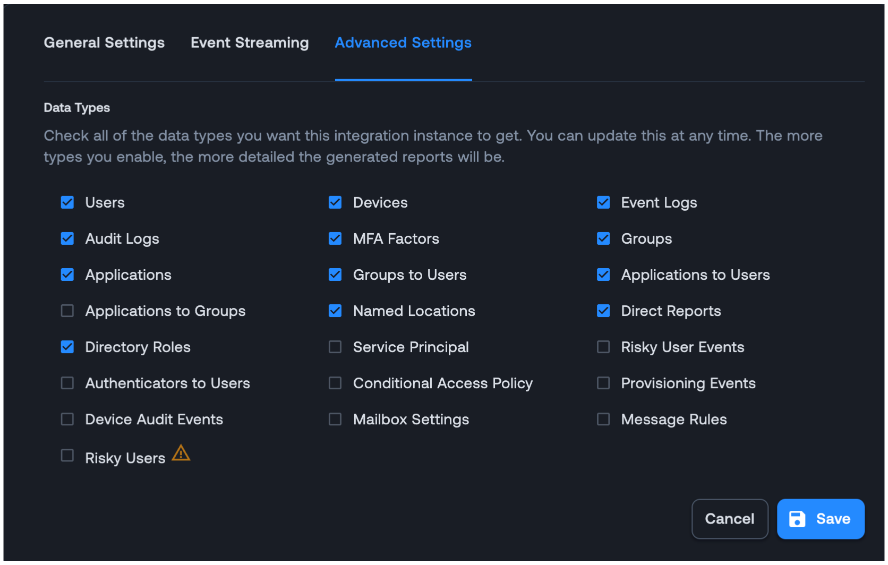
Oort has a range of turnkey integrations with identity sources, log stores, and productivity tools. This includes Microsoft Entra ID, but users can also bring in information from Okta, Auth0, Google Workspace, Workday, and Duo.

Step 2: Event Streaming

We recommended setting up event streaming from Azure Event Hub. This will ensure Oort provides comprehensive visibility into risk user events, event logs, and sign-in events.

Step 3: Configure Advanced Settings

Within the set-up process, users can define exactly what data Oort pulls in from Microsoft Entra ID. This includes users and groups, and Microsoft Entra ID Premium P2 customers will have access to additional data types.



Data Types

Check all of the data types you want this integration instance to get. You can update this at any time. The more types you enable, the more detailed the generated reports will be.

☑ Users
☑ Audit Logs
☑ Applications
□ Applications to Groups
☑ Directory Roles
□ Authenticators to Users
□ Device Audit Events
□ Risky Users ⚠

☑ Devices
☑ MFA Factors
☑ Groups to Users
☑ Named Locations
□ Service Principal
□ Conditional Access Policy
□ Mailbox Settings

☑ Event Logs
☑ Groups
☑ Applications to Users
☑ Direct Reports
□ Risky User Events
□ Provisioning Events
□ Message Rules

Step 4: Improve Hygiene

Organizations get immediate value. This includes easily identifying inactive accounts, MFA compliance issues, and visibility into who is using which applications.

Step 5: Identify Ongoing Threats

Oort continually monitors for weaknesses and threats associated with your identities. Regardless if you have joiners, leavers, or changes in contractors–you will always be able to identify behavioral anomalies, MFA weaknesses, IP threats, and much more.

Get in Touch

Contact us at sales@oort.io
Start your 30-day free trial: oort.io/demo