Oort Overview

Reduce the risk of account takeover

Prevent, detect, and respond to identity threats

With billions of exposed credentials and widespread weaknesses in MFA, most attackers have no need for malware; they simply log in. According to Verizon, credentials are cited to be responsible for over 80% of hacking related breaches.

Oort provides a protective layer on top of existing identity platforms and security teams a unique ability to detect identity threats and reduce organizations' identity attack surface.

The solution is cloud-native, agentless, easy to install, and integrates with your existing security tools.

Prevent
Oort proactively identifies potential weaknesses in your identity attack surface so you can avoid costly incidents.

Gain visibility into MFA usage, admin controls, unmanaged device access, over-permissioning, and more.

Detect
Continuously detect threats to identities, such as MFA flooding, Man in the Middle Attacks, session hijacking, impersonation, and risky email forwarding rules.

Oort pulls information from Okta Threat Intelligence and Microsoft Azure “Risky Users”.

Respond
Oort's rich, centralized context into user activity reduces investigation time by up to 80%.

Quickly report, remediate and recover with integrations into Slack, Teams, SIEM, SOAR, and ticketing platforms.

> Oort is very good at providing proactive alerts so incidents don't happen. The tool helps you work less in the middle of an emergency."
>
> **Dmitriy Sokolovskiy, CISO, Avid**

Key Benefits

- **Identify** impersonation and session hijacking attempts
- **Protect service accounts**, which can be privileged local or domain, or administrative accounts
- **Maintain compliance**, with NIST 800-63-3 by identifying MFA issues
- **Speed up investigations** by up to 80% with Oort's User 360.
- **Improve speed and safety** of password resets
- **Improve hygiene** of IAM program and save time identifying user inconsistencies and inactive users

How Oort Works

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 Your Integrations

Oort has a range of turnkey integrations with identity sources, log stores, and productivity tools. This includes Okta, Azure AD, Auth0, Google Workspace, Workday, and Duo. Oort extracts information on users, groups, apps, devices, authentication events, change logs, and threat information.

Step 2: Define Sensitive Applications

Tell us what applications are most sensitive to you and your organization's workflows. Events coming from the applications in the list will be marked as sensitive, helping you to align with your threat model and prioritize effectively.

Step 3: Configure Check Settings and Frequency

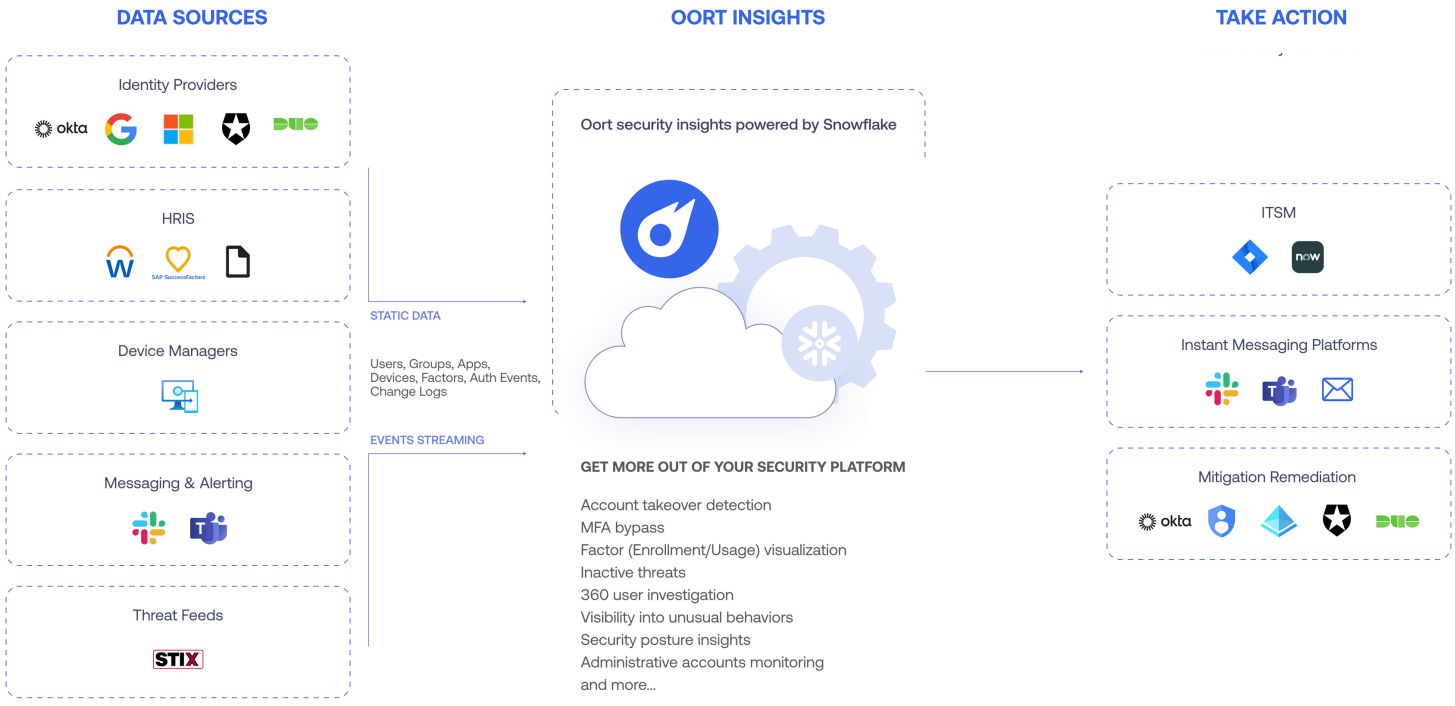
Oort has an extremely low false positive rate without the need to add any additional configuration or tuning. Users can add items to an ignore list, define custom grace periods, timing, and other customization options. This ensures the checks are fully tailored to you.

Step 4: Respond quickly to failing checks

Integrate with ServiceNow, Jira, Slack, Teams and other platforms to streamline respond. Alternatively, set up email notifications with custom messages to notify the necessary individuals or groups.

Step 5: Clean Up

Easily perform bulk clean-up actions within Oort, savings hours of work and improving the hygiene of your IAM program.



Why Oort?

Time to Value
Don't wait years until you get true insights. Plug-n-play integrations and out-of-the-box health checks can be provided in 30 minutes or less.

Proactive
Detecting identity threats is critical component of any identity security program. However, Oort goes even further by providing proactive and actionable insights into identity security posture management.

Multisource
Oort enables you to connect to any number of data sources to cover your entire identity fabric. With a platform powered by Snowflake, customers benefit from limitless historical event storage.

Support
Take advantage of our included unlimited support, training, and integration assistance.

"Oort allowed us to dramatically reduce time to investigate; you can easily change variables during and pivot laterally while still maintaining proper audit and traceability."

Myke Lyons, CISO, Collibra

"One of the quick advantages of Oort is that setting up took 60 or 90 minutes. We connected to Azure AD, MultiFactor Authentication System, ServiceNow and Microsoft Teams."

Harry Hoffman, CISO, Northeastern University

Get in Touch

Do you want to try Oort for free?

Want to see a customized demo?

Maybe you simply need some guidance with your AAD or Okta deployment?

You only need 15 minutes to see the Oort identity security platform in action. No intros, no nonsense, all identity threat detection and response.

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