Okta + Oort

Visibility and control for security teams

Prevent, detect, and respond to identity threats

Okta makes it easy for IT departments to deploy Single sign-on (SSO) and implement MFA, enabling your business to move faster to provision applications and access policies.

Unfortunately, security teams are often left in the dark when it comes to identity visibility, threat detection and response. Because identity a significant blindspot for security teams, attackers are increasingly targeting weaknesses in identities as part of their attacks.

With Oort, security teams benefit from comprehensive visibility and control over Okta. Oort provides continuous monitoring and visibility into their identity security without expensive scripting, custom rules, or log management.

Identity Threat Detection
Oort monitors activity, audit logs, and reported suspicious activity from Okta. Oort combines these insights with the inherent risk of each user based on how their account is configured and what applications they can access. This enables security teams to identify threats, such as session-hijacking, impersonation, and risky parallel sessions.

Reduce Identity Attack Surface
Beyond finding existing threats, Oort helps to reduce your identity attack surface. This includes MFA weaknesses, permission issues, and user inconsistencies. Improved cyber hygiene significantly reduces opportunities for attackers to exploit vulnerable accounts.

Effective Response
When Oort discovers weaknesses or threats, it can trigger a frictionless remediation workflow via Slack or Email. Furthermore, this can be integrated into ticketing, SIEMs, and other platforms.

Key Benefits

- **Identify** session hijacking attempts in Okta
- **Detect** admin impersonation in Okta
- **Secure** your organization's identities in Okta
- **Understand** users compliant with security controls
- **Detect** users exhibiting unusual or anomalous behavior
- **Speed** up threat investigations and incident response.
- **Simplify** the migration to Okta Identity Engine

Power Up Threat Investigations
Oort builds a User 360 profile for every identity in your population. Oort makes it fast and easy to search users from Okta and drill down into specific users during an investigation, reducing analyst workloads by as much as three hours per event.

Combine Okta with Additional Identity Sources
Users can integrate additional identity platforms, such as Microsoft Azure AD, to gain even more context to correlate with rich data from Okta. The Oort platform is powered by Snowflake, so customers benefit from limitless historical event storage.

"Oort is the only solution on the market that can identify session hijacking in Okta"

Dmitriy Sokolovskiy, CISO, Avid

Oort: A Security Layer On Top Of Okta

Extended Visibility, Additional Context, and Low False Positive

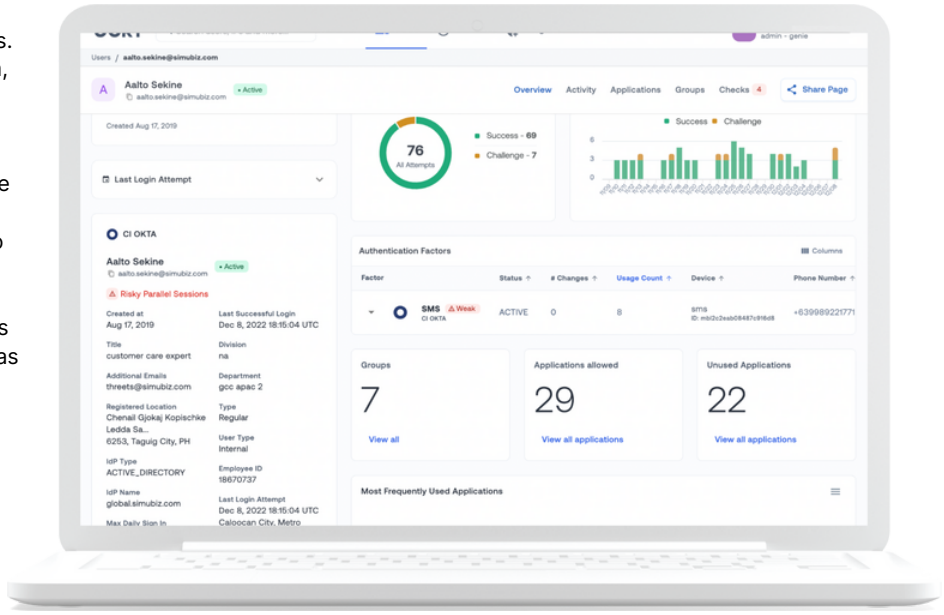
Oort seamlessly connects to your Okta instance to pull in a vast amount of data on users, groups, applications, and more.

Oort provides a layer of analysis on top of this data, helping to identify weaknesses and threats. These findings are available in the Oort platform, as well as in Slack, Teams, Email, Ticketing, or SIEM.

Want to create custom insights? No problem. We have more than 40 available out of the box, but you can always add more to further tune Oort to your organization's needs.

For even further insights, users can combine this information with data from other sources, such as Azure AD, Instant Messaging, and HR systems.

Security teams no longer need to be blind to identity risks.



okta

- Users
- Groups
- Policies
- Devices*
- Event Logs
- MFA Factors
- Applications
- Authenticators*

*Requires Okta Identity Engine

OORT

- MFA Coverage
- MFA Flooding
- Session Hijacking
- Inactive Account Probing
- Risky Parallel Session
- Admin Impersonation
- IP Threat
- Okta Session Length Policy Compliance

- Slack / Teams Workflows
- SIEM / SOAR Integration
- Automatic Ticketing

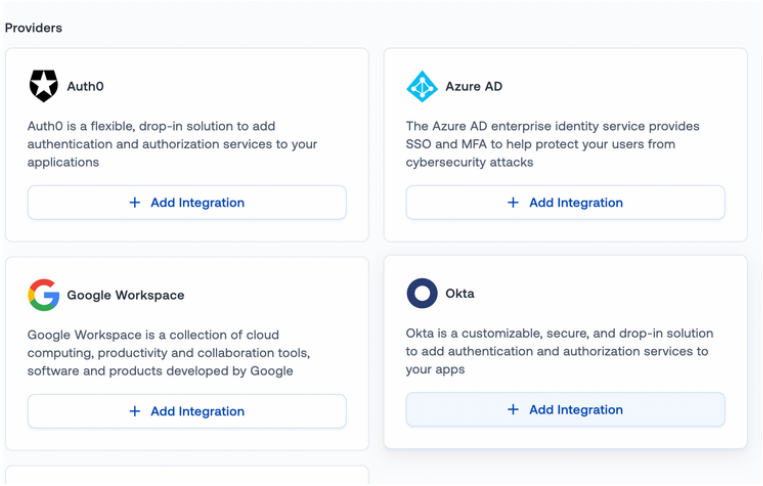
Getting Started

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 Okta, but users can also bring in information from 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: Configure Advanced Settings

Within the set-up process, users can define exactly what data Oort pulls in from Okta. This includes users, devices, event logs, applications, MFA factors. If you have Okta Identity Engine, you can also add device and authenticators information.

Step 3: Improve Hygiene

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

Step 4: 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 parallel sessions, session hijacking, MFA weaknesses, and much more.

Get in Touch

Do you want to try Oort for free?

Do you want to learn about identity security best practices, and what you peers are doing?

Want to see a customized demo?

Do you simply need some guidance with your Okta deployment?

If you think you could benefit from the visibility Oort provides, get in touch.

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

"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