

Intelligent AI-driven Identity Security



The time is now for organizations to adopt AI-driven identity security to stay ahead of security and compliance pitfalls. Digital transformation, the changing workforce, and an ongoing wave of compliance requirements have introduced so many users, points of access, applications and data that it has become almost overwhelming to IT departments to keep up. A human-based identity security approach can only scale so much, and with it comes error in identifying risk.

A new generation of identity driven by the power of AI is needed. One that enables identity to be autonomous while you stay in complete control. With the power of AI and machine learning, SailPoint Identity Platform helps organizations stay ahead of the security curve by proactively spotting risky users and access that pose potential threats. It learns and adapts as your organization changes so you can ensure that every user has the access they need when they need it. It connects and controls access to everything and everyone in the organization. Fundamentally it removes the complexity from identity and makes identity easy.



Anticipate
user access
needs



Spot risky
user
behaviors



Adapt and
automate
security policies



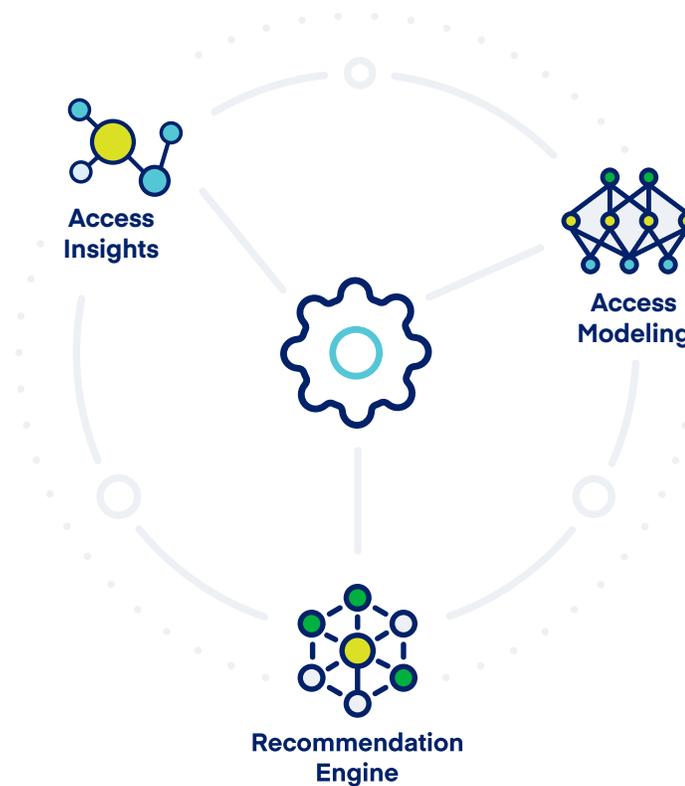
Connect and
control access
to everything

Enhance and Accelerate Identity

SailPoint Identity Platform is designed with AI-driven automation, machine learning and analytics, to remove complexity and empower your business to make intelligent, automated identity decisions.

With SailPoint Identity Platform AI Services, which includes Access Modeling, Access Insights and Recommendation Engine, you can:

- Analyze identity information to gain intelligence and actionable insights about your identity program
- Automate the creation and maintenance of new roles that align with the needs of your business
- Use recommendations to help decide what access should be requested, approved or removed





Access Insights

Access History

- Collect large amounts of access data, including roles that can be visualized in a more comprehensible format for analysis and reporting.
- Track and analyze user access over time from a single source of truth to provide complete visibility.
- Understand how access was granted and removed for better auditing.
- Identify patterns in user access to focus investigative efforts.
- Show the results of governance actions by correlating access changes to governance events.

Data Explore

- Collect identity data that can be visualized in a more consumable format for analysis and reporting.
- Query and filter by different access types, accounts, attribute changes, and governance events.
- Visualize and explore your identity data for tracking metrics and spotting trends.
- Evaluate the health of your identity security program using dynamic dashboards and charts.
- Create and customize dashboards and KPIs to showcase improvements made to your governance process.



Which means you can...

- Improve access visibility and awareness of improper or high risk access
- Accelerate the discovery of problematic access patterns
- Enable the development and sharing of KPIs to improve access analysis and investigation
- Demonstrate the effectiveness of your IGA program utilizing metrics with dashboards that can be shared with other stakeholders
- Support audit accuracy and compliance activity



Access Modeling

Role Fundamentals

- Start modeling access based on the needs of the organization.
- Utilize identity data as a starting point when kicking off your access modeling program.
- Understand how access is distributed throughout your organization by role.

Suggested Roles

- Visualize and modify potential roles using an intuitive UI that explains the data presented and allows for quick iterations.
- Identify clusters of like access that suggest a common role and who should be assigned.
- Analyze entitlements to understand the specific access to be included within the role and the make-up.

Role Insights

- Utilize continuous role analysis and suggestions to improve and maintain access models across the organization
- Understand if the access model is providing the right access within your role program.

Peer Group Analysis

- Use an automated patent-approved approach to build peer groups based on user attributes and access patterns.
- Discover similarities across identities utilizing peer group analysis and identity similarity metrics.



Which means you can...

- Eliminate the manual effort of analyzing user access
- Leverage automation to overcome the complexity and scale of access
- Align access to the needs of the business
- Create roles with the power of AI and machine learning
- Evaluate the effectiveness of your existing roles program
- Maintain your roles with AI and machine learning to ensure they stay current



Recommendation Engine

Access Certification Recommendations

- Simplify and shorten your access review cycle by providing approval recommendations for reviewers.
- Identify users who are outliers to the organization based on how their access compares to their peers.
- Utilize peer group analysis and identity attributes to help determine if access should be approved or removed.
- Review analysis details for each decision to reinforce automated decisions and understand the factors that contribute to a recommendation.

Access Request Recommendations

- Understand the reasons behind each recommendation decision based on peer group, location, role, and department.
- Automate the approval and provisioning of access for requests deemed low-risk to better focus on addressing high-risk access.
- Suggest additional access personalized to each identity.
- Reduce birthright permissions by relying on access recommendations to provide faster, more accurate incremental access decisions.
- Track and log recommended access actions for future audit and compliance support.



Which means you can...

- Alleviate certification fatigue that leads to incorrect access approvals
- Enable guidance for access and certification at the time of decision
- Accelerate the delivery of access to users
- Provide users with personalized access recommendations
- Improve governance efficiencies by automating low-risk IT tasks
- Prioritize focus on high risk user access

ABOUT SAILPOINT

SailPoint is the leader in identity security for the cloud enterprise. We're committed to protecting businesses from the inherent risk that comes with providing technology access across today's diverse and remote workforce. Our identity security solutions secure and enable thousands of companies worldwide, giving our customers unmatched visibility into the entirety of their digital workforce, and ensuring that each worker has the right access to do their job – no more, no less. With SailPoint as foundational to the security of their business, our customers can provision access with confidence, protect business assets at scale and ensure compliance with certainty.