ConductorOne

10 Best SailPoint Alternatives for Enterprise Identity Security

Legacy identity governance and administration (IGA) systems, like SailPoint, often present significant challenges due to prolonged implementation periods, substantial service costs, and cumbersome user experiences. Deployments can extend beyond a year, frequently requiring professional services that may double or triple the initial software investment. Additionally, integrating new applications and systems into these legacy platforms demands considerable effort, and their outdated interfaces can hinder user adoption and efficiency.

The good news is that legacy IGA isn't the only option. Modern IGA solutions like ConductorOne are designed to align with contemporary technological environments, offering rapid deployment and providing out-of-the-box integrations alongside open APIs for enhanced extensibility. With an emphasis on security, modern IGA solutions incorporate intelligent, risk-based access controls to effectively reduce standing privileges and bolster organizational security postures.

Why look for an alternative to SailPoint?

SailPoint is a legacy IGA platform built for a pre-cloud era. Here are a few reasons to look for an alternative to SailPoint:

- → **Long implementation times**: Deployments can take over a year
- → **High costs and hidden expenses**: Professional services can significantly add to software costs
- → **Unnecessary complexity**: Requires specialization to customize and has an outdated, frustrating UI
- → **Lack of innovation**: Limits visibility with outdated technology and doesn't address modern security needs

Key features and functionalities to consider in a SailPoint alternative

When researching SailPoint alternatives, it's essential to consider key features that align with your organization's needs and security posture. Here are some crucial aspects to keep in mind:

Comprehensive identity governance

→ **Identity lifecycle management**: The solution should automate the entire lifecycle of user identities, including provisioning, deprovisioning, and role management. This ensures that users have appropriate access only for the duration of their need.

→ **Access certification**: Regular reviews and certification of user access rights ensure compliance and minimize security risks. The tool should facilitate automated and streamlined certification campaigns.

→ **Segregation of duties (SoD)**: The tool should help you enforce SoD policies to prevent conflicts of interest and fraud by ensuring that no single user has excessive access privileges.

→ **Compliance management**: The alternative should support compliance with industry regulations and standards (e.g., GDPR, SOX, HIPAA) by providing audit trails, reporting, and risk assessment capabilities.

Integration capabilities and scalability

→ **Integration capabilities**: Seamlessly integrates with your existing IT infrastructure, including directories, applications, and cloud services.

→ **Scalability**: Scales to support organizational growth and evolving needs.

→ **Cloud support**: Supports hybrid and multi-cloud environments for diverse IT landscapes.

User experience and support

→ **User interface**: Simplifies user and administrator tasks to improve efficiency and adoption.

→ **Reporting and analytics**: Provides insights into user access, identifies risks, and tracks compliance.

→ **Vendor support**: Offers reliable support, documentation, and training resources.

Cost and value

→ **Pricing model**: Evaluate different pricing models (e.g., subscription, perpetual license) and choose the one that aligns with your budget and requirements.

→ **Total cost of ownership (TCO)**: Consider implementation, maintenance, and support costs in addition to the initial purchase price.

Top alternatives to SailPoint for IAM, user provisioning, and governance capabilities

1. **ConductorOne**
2. **Microsoft Entra Identity Governance**
3. **Lumos**
4. **Okta Identity Governance**
5. **Saviynt**
6. **IBM Security Verify Governance**
7. **Oracle Identity Governance**
8. **One Identity Manager**
9. **Omada**
10. **Ping Identity**

1. ConductorOne

ConductorOne is a cloud-native identity governance and administration (IGA) platform designed to simplify and automate identity security. It offers a user-friendly approach to managing access, particularly for hybrid environments that include SaaS and on-prem applications and modern and legacy infrastructure. With a focus on AI-powered automation and deep integrations, ConductorOne streamlines processes like access reviews, access controls, and lifecycle management. It prioritizes security with features like just-in-time access and risk-based alerts while empowering end users with self-service capabilities.

By combining a strong security posture with an intuitive interface, ConductorOne provides a modern alternative to traditional IGA solutions.

Key features

→ **Out-of-the-box and custom connectors**: Integrates in minutes with hundreds of cloud and on-prem applications. Easily configured generic connectors and a robust connector SDK enable quick integration of custom and homegrown systems.

→ **Unified Identity Graph**: Aggregates, normalizes, and visualizes granular access and identity data across cloud and on-premises systems, enabling comprehensive visibility and control over user permissions.

→ **Just-in-time access**: Reduces standing permissions by granting temporary access to applications and infrastructure only when needed, minimizing security risks while ensuring operational continuity.

→ **Automated access reviews**: Streamlines compliance by automating periodic and targeted access reviews, ensuring that permissions align with business needs and regulatory requirements without manual intervention.

→ **Copilot**: Leverages AI-powered insights to assist with decision-making in identity governance, such as recommending appropriate permissions or flagging anomalies in access patterns.

→ **Shadow IT detection**: Identifies unapproved applications and monitors unauthorized tool usage, providing actionable insights to enforce governance policies and mitigate risks.

→ **Separation of duties**: Tracks and identifies potential and existing access conflicts for proactive prevention and quick remediation.

→ **Identity lifecycle management**: Automates the management of identities throughout their lifecycle, from onboarding to offboarding, ensuring that access permissions remain appropriate at every stage.

→ **Slack integration**: Enables access requests, approvals, and review updates through Slack-based notifications and buttons.

Why do companies choose ConductorOne over SailPoint?

Compared to SailPoint, ConductorOne stands out as the stronger option due to the following:

→ **Faster deployment**: ConductorOne enables organizations to integrate systems within weeks, significantly reducing deployment times compared to SailPoint's often year-long implementations.

→ **Intuitive interface**: ConductorOne's design simplifies complex IAM tasks, enhancing user adoption and ensuring consistent security policy application.

→ **Modern capabilities**: ConductorOne incorporates AI-driven insights and just-in-time access provisioning, aligning with contemporary security needs.

→ **Transparent pricing**: ConductorOne offers clear, usage-based pricing without hidden costs, contrasting with SailPoint's additional expenses for professional services and complex contracts.

Here's what some users have been saying about ConductorOne:

"Being able to show ConductorOne to internal auditors for SOX compliance, where they can generate time-stamped, immutable reports, and see logs in one console, was impressive."

Jack Chen

SYSTEM1

Read Case Study → System1 saved over **90%** of time spent on access requests and reviews while reducing admin privileges and unused licenses.

"Having a tool that can do this in a timely fashion, iteratively and repeatedly, without manual inputs and outputs enables very real security control. This will improve our security posture."

Tim Lisko

DigitalOcean

Read Case Study → Digital Ocean automated UARs for SOC 2 and SOX audits and reduced effort by **85%**.

"ConductorOne is extremely customizable, very powerful, and doesn't make assumptions about how your organization works."

Matthew Sullivan

DigitalOcean

Read Case Study → Instacart moved **100%** of privileged access to automated, policy-based just-in-time (JIT) access with ConductorOne.

2. Microsoft Entra

Microsoft Entra is a comprehensive suite of IAM solutions designed to secure digital identities across an organization.

As part of Microsoft's ongoing commitment to identity security, Entra provides organizations with the tools (using Workload Identities) to authenticate, manage, and protect access to resources, applications, and environments. This ensures automated systems and IoT devices are authenticated and authorized, reducing potential attack vectors.

Key features

→ **Conditional access policies**: Enforces adaptive, context-aware access controls based on location, device health, and risk signals.

→ **Single sign-on (SSO)**: Simplifies access by allowing users to log into multiple apps with one set of credentials.

→ **Microsoft 365 integration**: Seamlessly manages identities and monitors activity across the Microsoft ecosystem.

Limitations

→ **Complex setup and configuration**: The setup and configuration process is complex and challenging for organizations without a dedicated IT team, consuming significant time and effort [*].

→ **High cost and complexity**: Some advanced features require paid subscriptions, increasing costs for larger organizations, and its integration with non-Microsoft applications can be complex and time-intensive [*].

→ **Limited support and resources**: Community support and resources for Spring Boot developers are limited, making it difficult to find specific security solutions or timely assistance during the development process [*].

Pricing

Microsoft Entra offers tiered pricing based on features and organizational needs. Plans start at $6 per user/month for Entra ID P1, with advanced capabilities available in Entra ID P2 at $9 and the full Entra Suite at $12 per user/month.

3. Lumos

Lumos is a modern SaaS access management platform that helps organizations track and control employee access to cloud applications. It gives companies real-time visibility into their system, automates access requests and approvals, and helps enforce least-privilege security principles.

In addition, Lumos connects with an organization's cloud applications to automatically discover and map all user permissions. It streamlines the access request process through an employee self-service portal, where users can request and managers can approve access based on roles and business needs.

Key features

→ **Automated permission mapping**: Connects to cloud apps to discover and map user permissions across the organization.

→ **Self-service access requests**: Empowers employees to request access and managers to approve based on roles and business needs.

→ **Intelligent access recommendations**: Suggests access levels using role and department data to reduce over-provisioning.

→ **Automated workflows**: Streamlines access reviews, offboarding, and license cleanup with built-in automation.

→ **Slack integration**: Enables quick actions and approvals through Slack-based notifications and buttons.

Limitations

→ **Complex interface**: Interface can be confusing at times, making it unclear what access users already have [*].

→ **Manual audits required**: Some application integrations are not fully connected to the one-click offboarding process, requiring manual audits [*].

→ **Difficult to understand**: Lumos has a steep learning curve, requiring intense effort to fully understand the software [*].

Pricing

Pricing not available. Please contact Lumos for more information.

4. Okta Identity Governance

Okta is a leading identity and access management solution that offers cloud-based solutions for secure access to applications and resources. Okta's identity governance product enables organizations to authorize access to applications, create lifecycle management workflows, and run access reviews.

Key features

→ **Lifecycle management**: Automates user onboarding and offboarding processes, ensuring efficient and secure identity management.

→ **Access reviews**: Automates access certification campaigns

→ **API access management**: Secures access to APIs, protecting sensitive data and services.

Limitations

→ **Lack of fine-grained visibility and control**: Users are provisioned access through groups, which limits visibility into fine-grained and effective access and the ability to assign, revoke, and review granular permissions.

→ **Limited connectivity**: Okta has limited integrations with on-prem systems and non-SCIM-enabled applications.

→ **High cost**: The pricing structure is steep for smaller companies, making it less accessible for businesses with limited budgets [*].

Pricing

Pricing not available. Please contact Okta for more information.

5. S Saviynt

Saviynt is an all-in-one platform that manages and secures user access across organizations. It combines identity governance, privileged access management (PAM), and application access control in a single system that works across cloud and on-site systems.

The platform features Identity-First Zero Trust, which checks every access request against security policies in real-time. Same as its Access Risk Exchange, which continuously evaluates risk by monitoring user behavior and system vulnerabilities.

Key features

→ **Out-of-the-box connectors**: Enables quick integration with enterprise systems and custom UIs through robust APIs.

→ **Application onboarding**: Simplifies onboarding, dynamic attribute management, and workflow design.

→ **Workflow automation**: Streamlines identity processes with flexible, low-code automation tools.

Limitations

→ **Limited capabilities**: Lacks SSO capabilities for integrated applications and flexible MFA enrollment options [*].

→ **Difficult upgrade process**: Despite the multi-tenant model, updates require extensive customer testing, often breaking existing functionalities, making the upgrade process difficult [*].

→ **Unfriendly UX**: Poor user experience particularly with the platform's user interface. For example, the small "View Detail" icon in the Entitlement tab is hard to locate [*].

Pricing

Pricing not available. Please contact Saviynt for more information.

6. IBM Security Verify Governance

IBM Security Verify Governance (ISVG) is a comprehensive IGA solution that enables organizations to manage user access, enforce compliance, and mitigate security risks in hybrid IT environments. Tailored for enterprises handling complex identity requirements, ISVG combines automation, analytics, and intuitive governance tools to streamline identity lifecycle management and ensure compliance with regulatory standards.

Key features

→ **Secure application access**: Provides seamless and secure logins across applications, with strong protection for sensitive data.

→ **Unified security integration**: Connects with other IAM solutions to create a cohesive security ecosystem.

→ **Lifecycle management**: Automates user onboarding and offboarding processes, ensuring efficient and secure identity management.

→ **API access management**: Secures access to APIs, protecting sensitive data and services.

Limitations

→ **High maintenance overhead**: Maintenance and updates for the platform can increase the total cost of ownership and demand significant resources [*].

→ **Limited role analysis and provisioning reliability**: Role analysis is overly simplistic, and access provisioning occasionally experiences errors, with some requests being missed [*].

→ **Skilled talent requirement for customization**: Custom connector development requires skilled engineers, which are harder to find for IBM products [*].

Pricing

Pricing not available. Please contact IBM for more information.

7. Oracle Identity Governance

Oracle Identity Governance solution drives enterprise-wide identity security through intelligent automation and risk-aware access controls.

The platform combines Identity Cloud Service (IDCS) with AI-powered workflows to handle everything from basic user access to complex role management. This is also combined with the platform's Connector Framework, which integrates with thousands of applications, from legacy systems to modern cloud services.

Key features

- → **Access orchestration**: Automates complex provisioning workflows and streamlines identity processes.
- → **Segregation of Duties (SoD)**: Prevents conflicting access rights by enforcing policy-based controls.
- → **Self-service identity management**: Enhances security with SSO, secure password resets, and user-friendly self-service tools.
- → **Scalable security**: Delivers stable performance and strong data protection across large environments.
- → **Automated provisioning**: Integrates with Oracle and third-party systems to simplify access and ensure compliance.

Limitations

- → **Limited customization capabilities**: Customization options are limited and do not always meet specific requirements, forcing reliance on out-of-the-box functionalities [*].
- → **Restricted workflow notifications**: Workflow and notification systems are limited to sending only three reminders, which may not be sufficient for some use cases [*].
- → **High complexity and cost**: The platform is complex to set up, has a steep learning curve, and its high costs, including implementation and maintenance, can be expensive for some organizations [*].

Pricing

Oracle doesn't offer exact pricing details of the plans. However, you can request a bill comparison to see if it's a fit for you.

8. One Identity Manager

One Identity Manager provides a unified governance framework that provides a single platform for managing identities, roles and access rights. It also supports deployment on both cloud and traditional systems, making it particularly effective for organizations with complex IT environments.

Key features

→ **Attestation automation**: Speeds up access reviews by prioritizing high-risk changes and streamlining low-risk renewals.

→ **Compliance dashboard**: Delivers real-time visibility into access violations for complex compliance needs.

→ **Role-based access control (RBAC)**: Simplifies RBAC setup with customizable scripts and intuitive field definitions.

→ **Unified identity view**: Centralizes identities and entitlements, with easy deactivation across systems.

Limitations

→ **Inconvenient password change process**: The database password change process, limited to every 42 days without user control, is inconvenient [*].

→ **Performance issues**: On-premise IDM upgrades can cause performance issues, impacting functionality [*].

→ **Complicated user experience**: Switching between environments (e.g., production vs. test) is complicated, with slow loading times and poor navigation [*].

Pricing

Pricing not available. Please contact One Identity for more information.

9. Omada

Omada's IGA solution combines identity lifecycle management, access governance, and compliance management in a user-friendly package. Its process-driven approach and strong focus on compliance, particularly with regulations like GDPR, make it a good fit for organizations seeking a streamlined and compliant IGA solution.

Key features

→ **IdentityPROCESS+ Framework**: Applies best practices to streamline identity governance based on years of industry experience.

→ **Smart connectors**: Easily integrate with existing business applications for seamless identity data flow.

→ **Assignment policies**: Automates access based on flexible criteria and supports GDPR surveys and multi-approver self-service flows.

→ **Centralized identity management**: Manages technical identities, SoD violations, account creation, and emergency lockouts from one platform.

→ **User-friendly interface**: Offers clean design, intuitive controls, and fast permission editing for efficient administration.

Limitations

→ **Complex error troubleshooting**: Troubleshooting errors can be overly complex, with limitations around editing certain objects, such as updating usernames linked to display names, leading to outdated data [*].

→ **Data handling limitations**: Lack of safety measures for HR data and no copy function for identity views [*].

→ **Survey overload**: The survey function can overwhelm managers with attestation questions [*].

Pricing

Pricing not available. Please contact Omada for more information.

10. Ping Identity

Ping Identity, through its unified PingOne Cloud Platform, unifies authentication, authorization, and intelligence capabilities. The platform's signature DaVinci orchestration engine streamlines identity workflows across cloud and on-premises environments, while PingIntelligence uses AI to detect and respond to suspicious access patterns.

Key features

→ **PingFederate**: Manages complex authentication flows and enables secure identity federation across enterprise environments.

→ **PingDirectory**: Provides a scalable directory service capable of managing billions of identities and attributes.

→ **Cloud-native scalability**: Adapts to business growth with flexible, cloud-based infrastructure.

→ **Advanced MFA**: Strengthens security with support for biometrics, smart cards, and other modern authentication methods.

→ **User-friendly configuration**: Easy to set up and manage, backed by a responsive and supportive team.

Limitations

→ **Disruptive user experience**: Frequent login session terminations are a recurring issue, disrupting user experience [*].

→ **High cost for advanced features**: Advanced features and functionalities in the premium tier are costly, making it less accessible for some organizations [*].

→ **Technical expertise required**: Custom policies for access management require technical expertise, adding complexity for less-experienced teams [*].

→ **High complexity**: Some interfaces, like PingAuthorize and PingDirectory, are overly complex and not user-friendly [*].

→ **Issues with software**: Software releases sometimes include bugs, leaving customers to report issues post-deployment [*].

Pricing

Pricing not available. Please contact Ping Identity for more information.

ConductorOne

ConductorOne – The Ideal SailPoint alternative

If your organization is still relying on legacy identity governance platforms like SailPoint, it's time to rethink your approach. **ConductorOne** is the modern alternative built for today's enterprises. While SailPoint deployments can take six to twelve months and often require costly professional services and extensive data preparation, ConductorOne gets customers fully deployed in under a month—with no hidden costs or heavy lift required.

If you're looking for a faster, simpler, and more secure way to manage identity governance, book a demo today to see how ConductorOne can transform your IGA program.

Try ConductorOne now

Get a demo

ConductorOne

AICPA SOC