ConductorOne

# 13 Best Identity Lifecycle Management Tools on the Market Right Now

## 1. ConductorOne

ConductorOne is a modern identity lifecycle management and governance platform designed to help organizations secure their workforce identities through automated access controls and governance.

ConductorOne centralizes identity management across various cloud and on-premises systems, providing a single source of truth for user access and permissions.

The platform emphasizes user experience and automation, making it easier for both IT and security teams to manage access, streamline compliance, and reduce the risk of identity-related breaches.

### What Makes ConductorOne Different?

ConductorOne reimagines identity lifecycle management by combining ease of use with proactive security. Unlike traditional, complex IGA solutions, ConductorOne prioritizes a user-friendly experience with self-service features and an intuitive interface. This empowers employees and reduces the burden on IT.

At the same time, ConductorOne leverages AI and automation to go beyond basic compliance, actively identifying and mitigating security risks. This unique blend of usability and security, coupled with its cloud-native design and agile development, makes ConductorOne a truly modern and effective solution for managing identities.

## Key Features

→ **Automated Access Reviews:** ConductorOne automates the process of regularly reviewing user access rights, ensuring that only authorized individuals have the necessary permissions. This helps to identify and mitigate access creep and enforce the principle of least privilege. It's simple to maintain compliance, reduce standing privileges, and enhance the organization's security posture without having to swim through spreadsheets. You can build workflows that meet your needs – highly configurable – and streamline certification. And there's a full audit trail so every step of the way is fully documented.

→ **Self-Service Access Requests:** Employees can request access to applications and resources through a user-friendly self-service portal. This reduces the burden on IT teams and speeds up the provisioning process. Imagine cutting your helpdesk tickets in half because employees can find the apps they want from a simple place, enabling them to easily request access via the web, Slack, or a developer-friendly command line. This access directory can also be fully integrated with a helpdesk, enhancing the ability to read, approve, and provision helpdesk access. Nor is this simply group memberships: fine-grained roles, permissions, and resources can be enabled, including pre-approved access.

→ **Automated Remediation:** ConductorOne can automatically revoke or modify access based on predefined policies or access review findings, reducing manual effort and improving security posture. The degree of flexibility is staggering: not tied to simply groups, ConductorOne's policies can be carefully fine-tuned to meet both simple and complex needs.

→ **Integration with Existing Systems:** The platform integrates with a wide range of cloud and on-premises applications, directories, and identity providers, allowing organizations to manage access across their entire IT ecosystem. Some popular ones include SaaS and cloud infrastructure such as directories, data warehouses, and HR systems, non-cloud infrastructure such as  LDAP, Postgres, Microsoft SQL, and more, and the ability to upload files directly or sync to S3 buckets for regular monitoring. You can also secure your on-premises technology such as Active Directory |and homegrown and back-office apps.

→ **Real-time Visibility and Reporting:** ConductorOne provides real-time visibility into user access and permissions, along with comprehensive reporting capabilities to support compliance audits. Like a GPS map, you can clearly see access paths for any user, application, or resource to get a better understanding of effective access and fine-grained permissions. When you confront problems such as orphaned accounts, inactive and high-risk users, and unused permissions, you can take action such as downgrading or revoking access and reassigning or removing accounts.

→ **Risk-Based Access Controls:** The platform analyzes user access and behavior to identify potential risks, such as orphaned accounts or excessive privileges, and alerts administrators to take corrective action. It allows users to surface risk indicators based on identity and permission levels. This is enabled through the power of AI: ConductorOne is able to guide users and suggest the actions to take based on an understanding of the organization's users, strategy, and exposure to risk.

### Why Do Companies Prefer ConductorOne?

→ *"When it comes to managing employee identities, C1 is our one-stop shop. We were able to fully implement C1 and have full adoption in under one week. Excellent documentation and a super helpful support team was a large part of the ease of set up. ConductorOne was there when we needed help, and gave us space when it was appropriate."* More from G2.

→ *"ConductorOne has made my fantasies of what Governance Management should look like a reality. The platform's user-friendly design allows us to consolidate all access requests into a single, streamlined system, eliminating the mess of this process smeared between emails, Jira tickets, and Slack messages."* More from G2.

→ *ConductorOne has proven to be an invaluable addition to our cybersecurity toolkit, enforcing the principle of least privilege has never been more straightforward. Its automation capabilities, combined with insightful risk analysis, have not only enhanced our security posture but have also saved us a ton of time and resources*. More from G2.

## 2. Microsoft Entra lifecycle management software

Microsoft Entra ID is a comprehensive identity and access management (IAM) solution that secures access to applications and resources across on-premises and multicloud environments. Tightly integrated with the Microsoft ecosystem, it offers seamless single sign-on, multi-factor authentication, and conditional access to protect against modern threats. Entra ID simplifies identity governance with automated provisioning, access reviews, and entitlement management.

### Key Features

→ **Conditional Access:** Enforces granular access policies based on user context, device state, and application sensitivity. This allows organizations to dynamically control access and mitigate risks in real-time.

→ **Azure AD Connect:** Synchronizes on-premises identities with Azure AD, enabling hybrid identity management and seamless access to cloud resources.

→ **Identity Protection:** Detects and remediates identity-related risks like compromised credentials, suspicious sign-in attempts, and leaked credentials.

### What are some limitations of Microsoft Entra?

→ *"Various features that can be complex to set up and manage, especially for organizations with limited IT resources. Integrating Entra ID with some non-Microsoft applications requires additional configuration."* More from G2.

→ *"You need an entire IT department just to understand and set it up. Way too complex for any company with less than a few hundred employees."* More from G2.

→ *"Too much management, and very little automation makes the additional tasks required tedious. Also, if you are not an AD savvy person, it can be difficult to understand."* More from G2.

## Pricing

Microsoft Entra is priced at $10.40 per resource per month.

# 3. Okta Lifecycle Management

Okta is a leading independent identity provider that connects people to technology securely. Its platform enables single sign-on, multi-factor authentication, and lifecycle management for workforce and customer identities. Okta integrates with a vast network of applications, offering seamless and secure access across diverse IT environments.

## Key Features

- **Universal Directory:** A centralized cloud-based directory that stores and manages all user identities, attributes, and access rights.
- **Adaptive Multi-Factor Authentication:** Provides strong authentication with various factors, adapting to user context and risk levels.
- **Lifecycle Management:** Automates user onboarding, provisioning, and offboarding across applications and systems.

## What are some limitations of Okta?

- *"The UI is often confusing -- you can't tell which items are generic services where you have to save your own password vs ones where the company has set them up for you."* More from G2.
- *"The setup and log-in processes are tedious and confusing. It usually takes my group 15 minutes to log in."* More from G2.
- *"It's very frustrating to not have an email option to approve logging in. We are only able to verify signing in on our phones."* More from G2.

## Pricing

Okta has 15 different pricing plans, beginning at $1,500 for smaller businesses.

# 4. SailPoint Lifecycle Management

SailPoint is a comprehensive identity security platform that provides visibility and control over user access. Its solutions automate identity governance processes, such as access certifications, provisioning, and policy enforcement. SailPoint leverages AI and machine learning to identify and mitigate access risks, ensuring compliance and reducing the attack surface.

### Key Features

→ **IdentityIQ:** A robust identity governance and administration (IGA) solution that automates access requests, certifications, and policy enforcement.

→ **Predictive Identity:** Uses AI and machine learning to analyze user access behavior and identify potential risks before they become breaches.

→ **Access Modeling:** Simulates the impact of access changes before they are implemented, helping organizations avoid unintended consequences.

### What are some limitations of Sailpoint?

→ *"The user interface is not friendly."* More from G2.

→ *"The installation process of Sailpoint was very difficult for me."* More from G2.

→ *"The cache issue is a very common issue in Sailpoint."* More from G2.

### Pricing

Sailpoint pricing starts at $10/user per month for the basic edition.

## 5. CyberArk Lifecycle Management

CyberArk focuses on protecting privileged access, which is a critical aspect of identity security. It offers a comprehensive solution for managing, monitoring, and securing privileged accounts and credentials. By securing these high-risk accounts, CyberArk helps organizations prevent unauthorized access to sensitive systems and data, reducing the risk of breaches and insider threats.

### Key Features

→ **Privileged Access Manager:** Secures, manages, and monitors privileged accounts, including shared accounts, application credentials, and SSH keys.

→ **Application Access Manager:** Secures access to applications and systems by managing credentials and enforcing least privilege.

→ **Secrets Management:** Secures and manages secrets, such as API keys, encryption keys, and certificates, protecting sensitive data and configurations.

### What are some limitations of CyberArk?

→ Explain in bullet points, one simple sentence per bullet

→ *"Performance issues with large deployments. Requests could repeatedly fail or refuse to execute at all when dealing with large pool of data."* More from G2.

→ *"HIgh initial friction to get familiar with the platform."* More from G2.

→ *"The solution is complex and requires professional services to just deploy the solution."* More from G2.

## Pricing

Cyberark pricing is not publicly available.

# 6. Auth0 User Management

Auth0 provides a universal identity platform that enables organizations to manage customer identities and secure access to applications. It offers a wide range of features, including authentication, authorization, user management, and single sign-on. Auth0 simplifies identity management for developers, allowing them to easily integrate authentication and authorization into their applications.

## Key Features

→ **Universal Login:** Provides a customizable login experience for users, supporting various authentication methods and social logins.

→ **User Management:** Offers a centralized platform for managing user profiles, roles, and permissions.

→ **Authorization:** Enables fine-grained access control to applications and APIs based on user roles and attributes.

## What are some limitations of Auth0 User Management?

→ *"The customer support is truly abysmal."* More from G2.

→ *"They are super expensive; it could look like decent pricing, but when you consider that they deliver no support and have operational issues, I would say they are overpriced."* More from G2.

→ *"The documentation is awful, and there's many bugs in the SDKs they provide."* More from G2.

## Pricing

Auth0's pricing starts at $35/month.

# 7. Microsoft Azure Active Directory

Azure AD is Microsoft's cloud identity and access management service. It provides a centralized platform for managing user identities and access to applications and resources. Azure AD offers a range of features, including single sign-on, multi-factor authentication, and conditional access. It seamlessly integrates with other Microsoft services and supports hybrid identity scenarios.

## Key Features

- **Single Sign-On:** Enables users to access multiple applications with a single set of credentials.
- **Multi-Factor Authentication:** Adds an extra layer of security by requiring users to verify their identity with multiple factors.
- **Conditional Access:** Enforces granular access policies based on user context, device state, and application sensitivity.

## What are some limitations of Microsoft Azure Active Directory?

- *"It has a really confusing interface sometimes."* More from G2.
- *"It's very slow in performance."* More from G2.
- *"Policies can take some time to sync with users' computers when group policy is changed."* More from G2.

## Pricing

The pricing for Microsoft Azure AD starts at $6.00 per user per month.

# 8. Ping Identity PingOne For Workforce

PingOne for Workforce provides a cloud-based identity and access management solution that simplifies and secures workforce access to applications. It offers features like single sign-on, multi-factor authentication, and directory federation, enabling employees to seamlessly access the resources they need. PingOne for Workforce also supports passwordless authentication and risk-based adaptive authentication, enhancing security and user experience.

## Key Features

- **PingID:** Provides strong authentication with various factors, including push notifications, biometrics, and one-time passwords.
- **Directory Federation:** Connects with existing on-premises directories like Active Directory, allowing organizations to leverage their existing identity infrastructure.
- **Passwordless Authentication:** Enables users to authenticate without passwords, improving security and convenience.

## What are some limitations of Ping Identity PingOne?

- *"Very difficult to integrate with our complex environment."* More from G2.
- *"Extremely steep learning curve."* More from G2.
- *"Ping Identity documentation needs improvement."* More from G2.

### Pricing

Ping Identity starts at $20,000 annually.

## 9. Oracle Identity and Access Management

Oracle Identity Management offers a comprehensive suite of identity governance and administration (IGA) solutions that help organizations manage and secure user identities across on-premises and cloud environments. It provides features like identity lifecycle management, access management, and directory services. Oracle Identity Management helps organizations comply with regulatory requirements and reduce the risk of unauthorized access.

### Key Features

→ **Oracle Identity Governance:** Automates access certifications, provisioning, and policy enforcement to streamline identity governance processes.

→ **Oracle Access Manager:** Secures access to applications and resources with features like single sign-on, multi-factor authentication, and authorization.

→ **Oracle Unified Directory:** Provides a centralized directory service for managing user identities and attributes.

### What are some limitations of Oracle Identity and Access Management?

→ *"Installation is too complicated."* More from G2.

→ *"Updates/upgrades are very complex, brittle, and difficult."* More from G2.

→ *"It is challenging to manage."* More from G2.

### Pricing

Cyberark pricing is not publicly available.

## 10. Symantec (now part of Broadcom)

Symantec (now part of Broadcom) offers a range of identity security solutions that protect against cyber threats and secure access to critical assets. Its solutions include identity governance and administration (IGA), privileged access management (PAM), and customer identity and access management (CIAM). Symantec helps organizations manage and secure identities across their entire ecosystem, reducing the risk of breaches and compliance violations.

## Key Features

→ **Symantec Identity Governance:** Automates access certifications, provisioning, and policy enforcement to streamline identity governance processes.

→ **Symantec Privileged Access Manager:** Secures, manages, and monitors privileged accounts to prevent unauthorized access to sensitive systems.

→ **Symantec VIP:** Provides strong authentication with various factors, including one-time passwords and push notifications.

## What are some limitations of Symantec?

*Explain in bullet points, one simple sentence per bullet*

→ *"Good luck trying to renew after Broadcom took over."* More from G2.

→ *"The management system is a nightmare to navigate."* More from G2.

→ *"The user interface is ancient."* More from G2.

## Pricing

Symantec pricing is not publicly available.

# 11. ForgeRock Identity Platform

ForgeRock provides a comprehensive identity and access management (IAM) platform that helps organizations manage and secure identities across various applications and devices. It offers a modular and flexible architecture, allowing organizations to tailor the platform to their specific needs. ForgeRock supports modern authentication standards and protocols, enabling secure access to cloud, mobile, and IoT applications.

## Key Features

→ **Identity Management:** Provides a centralized platform for managing user identities, attributes, and access rights.

→ **Access Management:** Secures access to applications and resources with features like authentication, authorization, and single sign-on.

→ **Directory Services:** Offers a scalable and secure directory service for storing and managing user identities and attributes.

## What are some limitations of ForgeRock Identity Platform?

→ *"Subscription cost is too high."* More on G2.

→ *"Navigating the settings isn't easy if you don't know exactly what you're looking for."* More on G2.

→ *"They should improve reporting for audit purposes."* More on G2.

### Pricing

Explain the pricing in 2-3 sentences if the information is publicly available.

## 12. JumpCloud Identity Lifecycle Management

JumpCloud offers a cloud-based directory platform that simplifies identity and access management for organizations. It provides a centralized platform for managing users, devices, and applications. JumpCloud supports various authentication methods, including passwordless authentication, and offers automated user provisioning and deprovisioning.

### Key Features

→ **Cloud Directory:** A centralized cloud-based directory that stores and manages user identities, attributes, and access rights.

→ **Device Management:** Manages and secures devices, including laptops, desktops, and mobile devices.

→ **Single Sign-On:** Enables users to access multiple applications with a single set of credentials.

### What are some limitations of JumpCloud?

→ *"You need to know scripting to be able to write scripts to pull reports."* More on G2.

→ *"The licensing model is a bit of a drawback."* More on G2.

→ *"Jumpcloud should come up with advanced features like Identity access governance features like recertifications to application access with time-limited access policies."* More on G2.

### Pricing

Jumpcloud's lowest edition, for device management only, starts at $9 per user per month.

## 13. OneLogin Identity Lifecycle Management

OneLogin provides a cloud-based identity and access management (IAM) solution that simplifies user provisioning and access control. It offers a centralized platform for managing users, applications, and roles. OneLogin supports single sign-on, multi-factor authentication, and automated user provisioning and deprovisioning.

## Key Features

Just the most important ones, one simple sentence per bullet.

- **Unified Access:** Provides a single point of access to all applications, both on-premises and in the cloud.
- **Adaptive Authentication:** Enforces risk-based authentication policies based on user context and behavior.
- **User Provisioning:** Automates user onboarding and offboarding across applications and systems.

## What are some limitations of OneLogin?

*Explain in bullet points, one simple sentence per bullet*

- *"In order to realize any benefits it is necessary to purchase the highest tier."* More on G2.
- *"Documentation is out of date."* More on G2.
- *"The UI is confusing."* More on G2.

## Pricing

Pricing starts at $6 per user per month.

# Identity Lifecycle Management (FAQs)

## What Is Identity Lifecycle Management (ILM)?

Identity Lifecycle Management (ILM) is the comprehensive process of managing digital identities throughout their entire lifecycle within an organization. This includes everything from the initial creation of an identity (e.g., when an employee joins) to modifying access as their role changes, and ultimately to deactivating or deleting the identity when it's no longer needed (e.g., when an employee leaves).

Think of it as the HR process for digital identities. Just like employees go through onboarding, promotions, and offboarding, digital identities need to be managed through their various stages to ensure appropriate access and security.

## How Does Identity Lifecycle Management Work?

ILM typically involves these key stages:

- **Provisioning:** Creating new identities and granting initial access rights based on the user's role and responsibilities. This often involves integrating with HR systems to automate the process when a new employee joins.
- **Access Management:** Managing and controlling access to resources and applications based on defined policies and roles. This includes granting, modifying, and revoking access as needed.
- **Access Review:** Regularly reviewing user access rights to ensure they are still appropriate and aligned with the principle of least privilege. This helps prevent access creep and identify potential security risks.
- **Deprovisioning:** Deactivating or deleting identities when they are no longer needed. This is crucial to prevent unauthorized access from former employees or contractors.

ILM solutions often employ automation and AI to streamline these processes, improve efficiency, and enhance security. They also provide centralized visibility and control over all identities and access rights, helping organizations meet compliance requirements and reduce the risk of breaches.

## Key Features to Look for in an IAM Solution

- **Automated Provisioning and Deprovisioning:** Streamlines the creation and deletion of user accounts and access rights, ensuring efficient onboarding and offboarding processes.
- **Access Certification:** Automates the process of regularly reviewing user access rights to ensure they are appropriate and comply with policies.
- **Role-Based Access Control (RBAC):** Allows you to define roles with specific permissions and assign users to those roles, simplifying access management and enforcement.
- **Self-Service Capabilities:** Empowers users to manage their own access, such as requesting access to resources or resetting passwords, reducing the burden on IT.
- **Multi-Factor Authentication (MFA):** Enhances security by requiring users to verify their identity with multiple factors, such as a password and a one-time code.

→ **Integration with Existing Systems:** Ensures seamless integration with your existing HR systems, directories, and applications for efficient data flow and management.

→ **Reporting and Analytics:** Provides insights into user access, activity, and potential risks, helping you identify and address security vulnerabilities.

→ **Compliance Support:** Helps you meet regulatory requirements and industry standards by providing audit trails, access certifications, and other compliance-related features.

## Key Benefits of Using IAM Tools

→ **Improved Security:** Reduces the risk of unauthorized access and data breaches by enforcing strong authentication, access controls, and identity governance.

→ **Increased Efficiency:** Automates identity-related tasks, such as provisioning and access reviews, freeing up IT resources and improving productivity.

→ **Reduced Costs:** Eliminates manual processes and reduces the need for IT support, leading to cost savings.

→ **Enhanced Compliance:** Helps organizations comply with regulatory requirements and industry standards, avoiding penalties and reputational damage.

→ **Centralized Control:** Provides a single point of control for managing all identities and access rights, simplifying administration and improving visibility.

→ **Better Decision-Making:** Provides insights into user access and activity, enabling informed decisions about security and access management.

# Talk to our team.

Or take a self-guided tour to learn more!

Try ConductorOne now

Get a demo

ConductorOne | team@conductorone.com

AICPA SOC