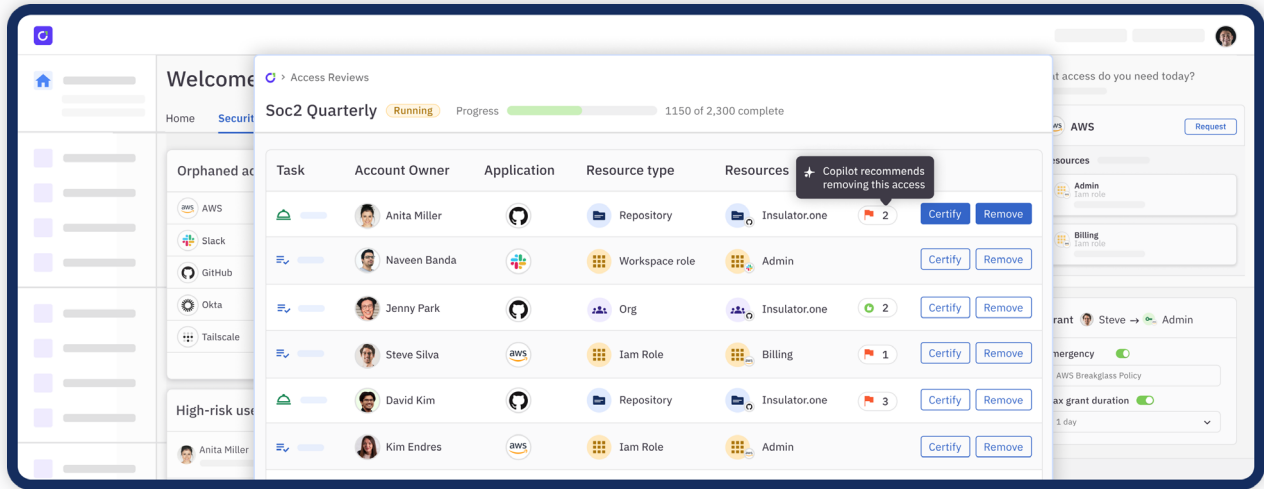


10 Best Identity and Access Management (IAM) Tools Right Now



Why are IAM tools important? As organizations grow, so does the complexity of managing user access. IAM tools are designed to scale with the organization, handling an increasing number of user identities and integrations with new applications and services. This scalability ensures that the security posture grows stronger and more comprehensive as the organization expands.

1. ConductorOne



[ConductorOne](#) is an identity security solution designed to streamline and secure access management processes in organizations. The platform specializes in automating identity lifecycle management, focusing on minimizing risks associated with excessive or inappropriate access rights. It integrates seamlessly with existing identity providers (IdPs) and infrastructure as code (IaC) environments, making it a flexible option for modern enterprises.

ConductorOne's capabilities include automated [access reviews](#), [just-in-time provisioning](#), intelligent [access controls](#), and an access [Copilot](#) that leverages machine learning to suggest appropriate access levels based on user behavior and role requirements.

A key feature of ConductorOne is its user-friendly interface, which simplifies the management of complex permissions and audit processes.

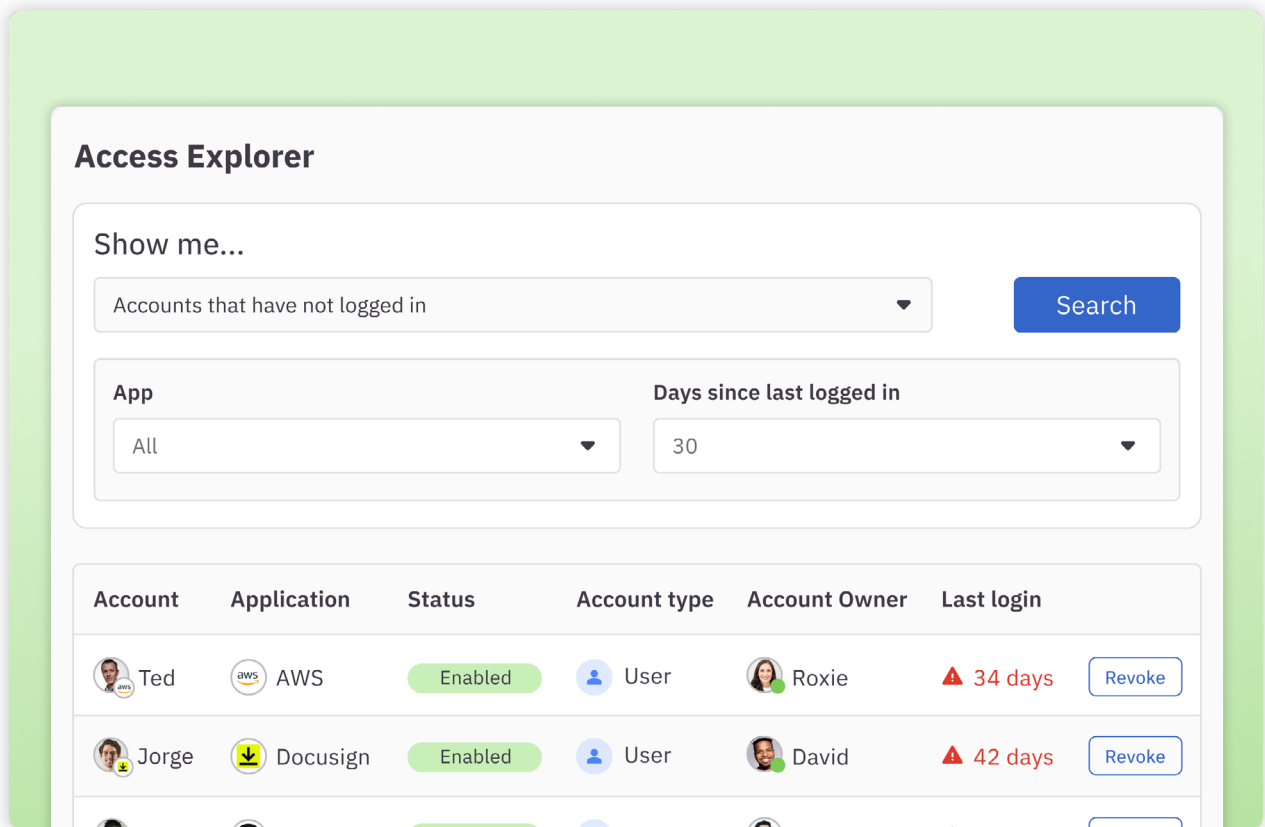
The platform also offers detailed analytics and reporting features, providing insights into access patterns and potential security vulnerabilities. This enables IT teams to make informed decisions quickly, enhancing overall security posture with minimal manual intervention.

Key Features of ConductorOne

Comprehensive Identity Management Dashboard

ConductorOne offers a centralized dashboard built upon its innovative [Access Fabric](#), which centralizes and unifies identity and access data from multiple sources including cloud and on-prem apps, directories, and infrastructure.

This comprehensive view provides users with full visibility and control as well as powerful search capabilities and visualization tools that quickly highlight access risks and insights.



Automated Access Review and Compliance Reporting

ConductorOne streamlines the process of access certifications and compliance reporting, making it a top choice for organizations focused on maintaining rigorous security standards.

Organizations can customize user access reviews with multistep reviewer policies and integrate real-time notifications via Slack for review processes, auto-approvals, and zero-touch deprovisioning.











In addition, the platform enables you to generate accurate, auditor-ready reports with just a single click, significantly reducing the administrative burden on IT teams.

Soc2 Quarterly Q4 FY23 Completed

2,300 of 2,300 complete

Approved: 2,170 | Denied: 127 | Skipped: 3

Search [] App [] Status: Approved, Denied [] Risk level [] Compliance Framework []

App Identity	Type	Entitlements	Policy	Decision	Outcome
 Perry perry@acmecocom	User	 gcp-security-admins Google Workspace . Groups Member	<u>Security policy</u>	Denied Oct 15	Access revoked
 Ben ben@acmecocom	User	 gcp-devops Google Workspace . Groups Member	<u>Two step policy</u>	Approved Oct 15	-
 Sue sue@acmecocom	User	 AdminAccess AWS . Iam Role	<u>Manager policy</u>	Approved Oct 15	-
 Danielle danielle@acmecocom	User	 gcp-devops Google Workspace . Groups Member	<u>On call policy</u>	Approved Oct 15	-
 Harvey harvey@acmecocom	User	 AdminAccess AWS . Iam Role	<u>Manager policy</u>	Approved Oct 15	-

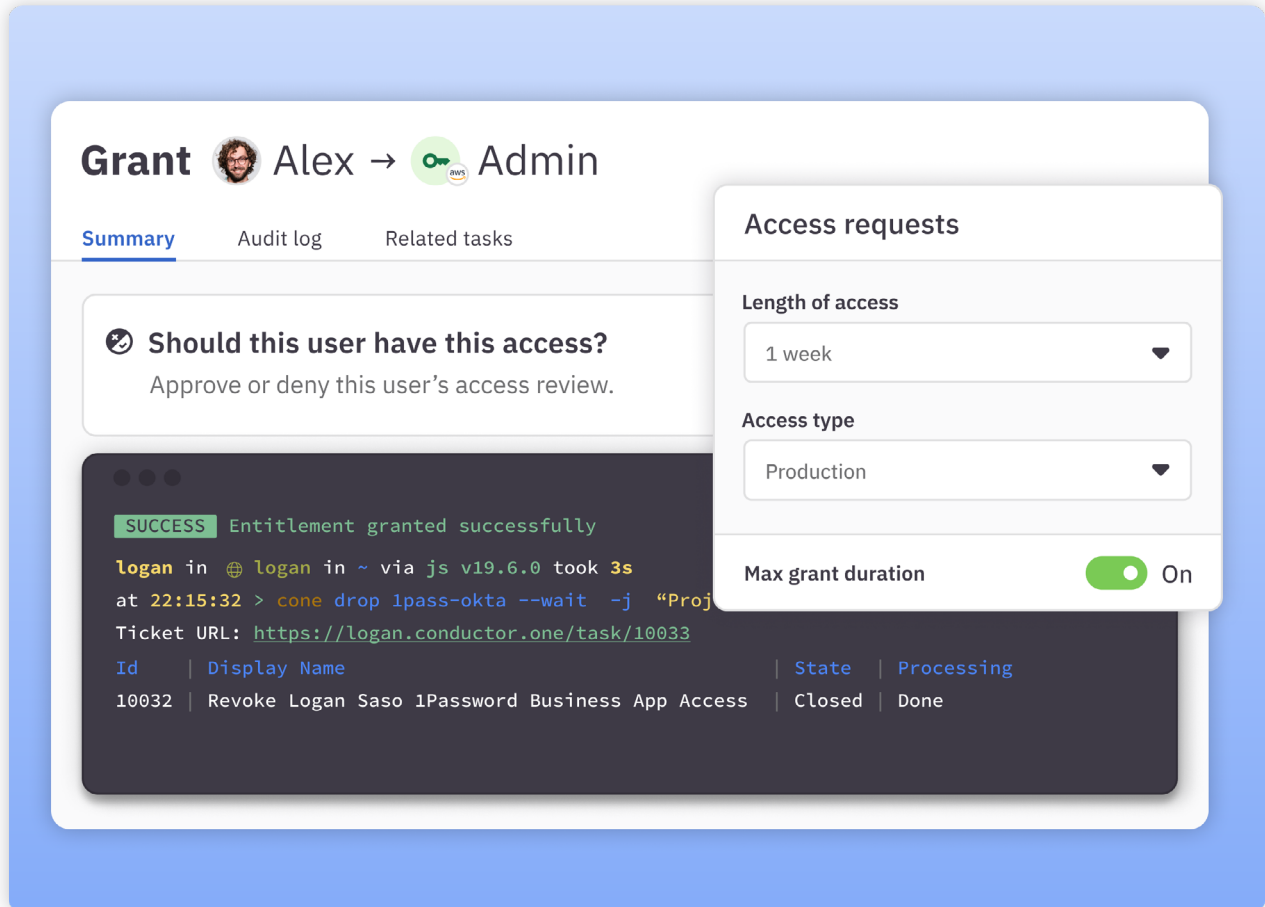
5 of 2,300

 [Learn more about access reviews →](#)

Just-in-Time Provisioning and Self-Service Access Requests

ConductorOne enhances user autonomy by enabling self-service access requests through various interfaces like Slack, CLI, or web app, paired with automatic provisioning upon approval.

Customers can easily set up self-requested just-in-time access to any resource to support a zero standing privileges policy, which can significantly reduce security risks by ensuring that access rights are granted only as needed and for a limited time.



The screenshot displays the ConductorOne interface for reviewing a grant. At the top, it shows 'Grant Alex → Admin'. Below this are tabs for 'Summary', 'Audit log', and 'Related tasks'. The main content area features a question: 'Should this user have this access?' with the instruction 'Approve or deny this user's access review.' Below the question is a terminal window showing a successful command execution: 'logan in @ logan in ~ via js v19.6.0 took 3s at 22:15:32 > cone drop lpass-okta --wait -j "Proj" Ticket URL: https://logan.conductor.one/task/10033'. A table below the terminal shows the task details:

Id	Display Name	State	Processing
10032	Revoke Logan Saso 1Password Business App Access	Closed	Done

On the right side, there is a sidebar titled 'Access requests' with the following settings:













- Length of access: 1 week
- Access type: Production
- Max grant duration: On

[🔗 Learn more about JIT access →](#)

Lifecycle Identity Management

The platform automates every phase of the identity lifecycle, from onboarding to offboarding. Features include multi-step [provisioning and deprovisioning](#) workflows and the management of delegated requests.

It also provides tools for detecting and revoking unused access, orphaned accounts, and deactivated users to keep the system clean and secure.

Account	Application	Status	
 Roxie roxie@acmecocom	 AWS	Orphaned	Revoke
 David davif@acmecocom	 DocuSign	Enabled	Revoke
 Naveen naveem@acmecocom	 Github	Enabled	Revoke
 Peter peter@acmecocom	 Google Workspace	Suspended	Revoke
 Jenny jenny@acmecocom	 Okta	Enabled	Revoke
 Mary mary@acmecocom	 Slack	Enabled	Revoke

 [Learn more about access management →](#)

Enforce Separation of Duties

ConductorOne's automated detection of SoD conflicts across applications ensures that internal security controls meet stringent compliance standards. It alerts administrators to conflicts, offers remediation options, and logs activities for audits.



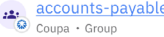














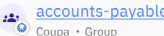
Financial Authorization Conflicts

Enable this conflict monitor when you're done making changes Enable

Once your conflict monitor is ready, click "Enable" to put it into action.

[Alerts](#) [Settings](#)

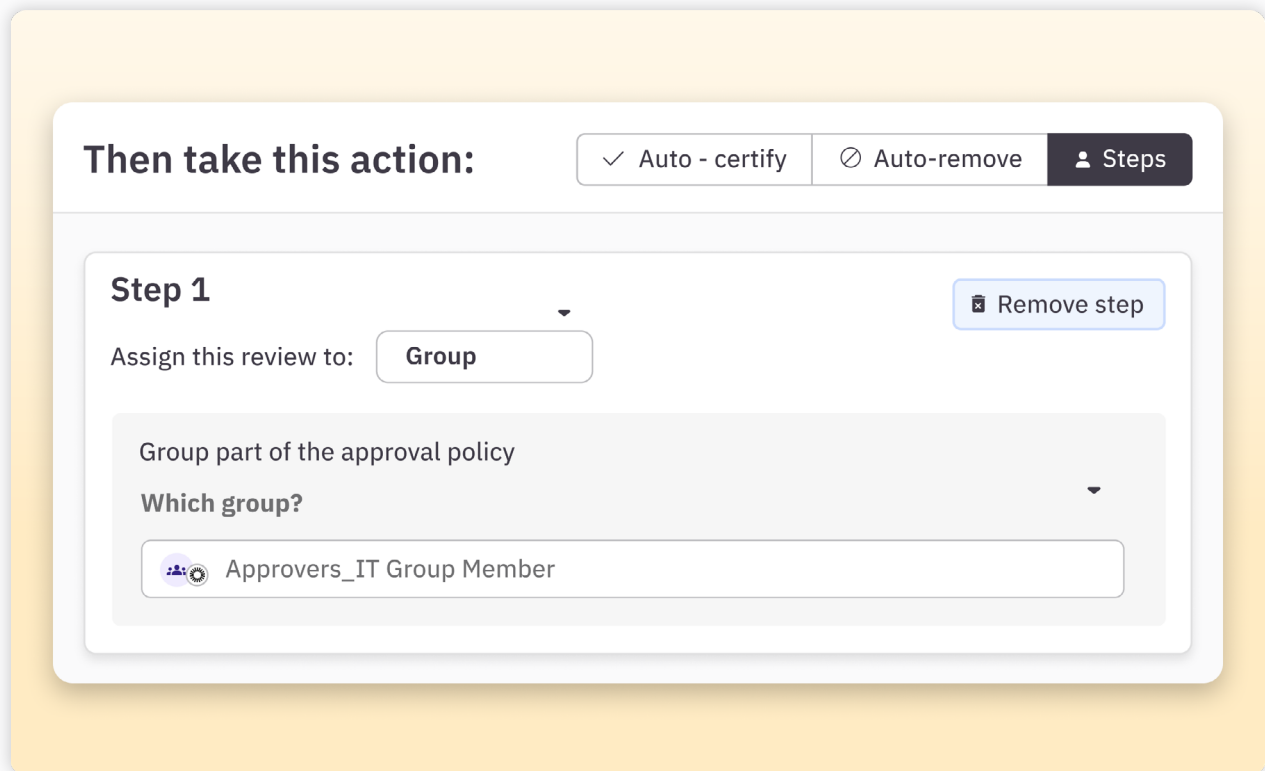
Entitlement ⌵ ⌵

Account owner	Conflict	Detected on	Status
 Jack Shaal	 + 	May 10	Exempted Exempt ...
 Sue Park	 + 	May 10	Active Exempt ...
 Elijah Davis	 + 	May 10	Active Exempt ...
 Hannah Moore	 + 	May 10	Active Exempt ...
 Oliver Tran	 + 	May 10	Exempt ...
 Harvey Lopez	 + 	May 10	Active Exempt ...

Policy-Driven Access Controls

ConductorOne offers advanced policy-driven access controls that attract organizations looking for dynamic and secure access management solutions.

Users can set up zero-touch, conditional, and multi-step approval policies, automatically remove access based on specific triggers such as time, non-usage, or changed justifications, and require re-requesting for particularly risky access permissions.



The screenshot displays a configuration interface for a policy action. At the top, the heading "Then take this action:" is followed by three tabs: "Auto - certify" (checked), "Auto-remove", and "Steps" (selected). Below this, a "Step 1" configuration box is shown. It includes a "Remove step" button, a label "Assign this review to:" with a "Group" dropdown, and a section titled "Group part of the approval policy" with a "Which group?" dropdown. The selected group is "Approvers_IT Group Member".

Then take this action: Auto - certify Auto-remove **Steps**

Step 1 Remove step

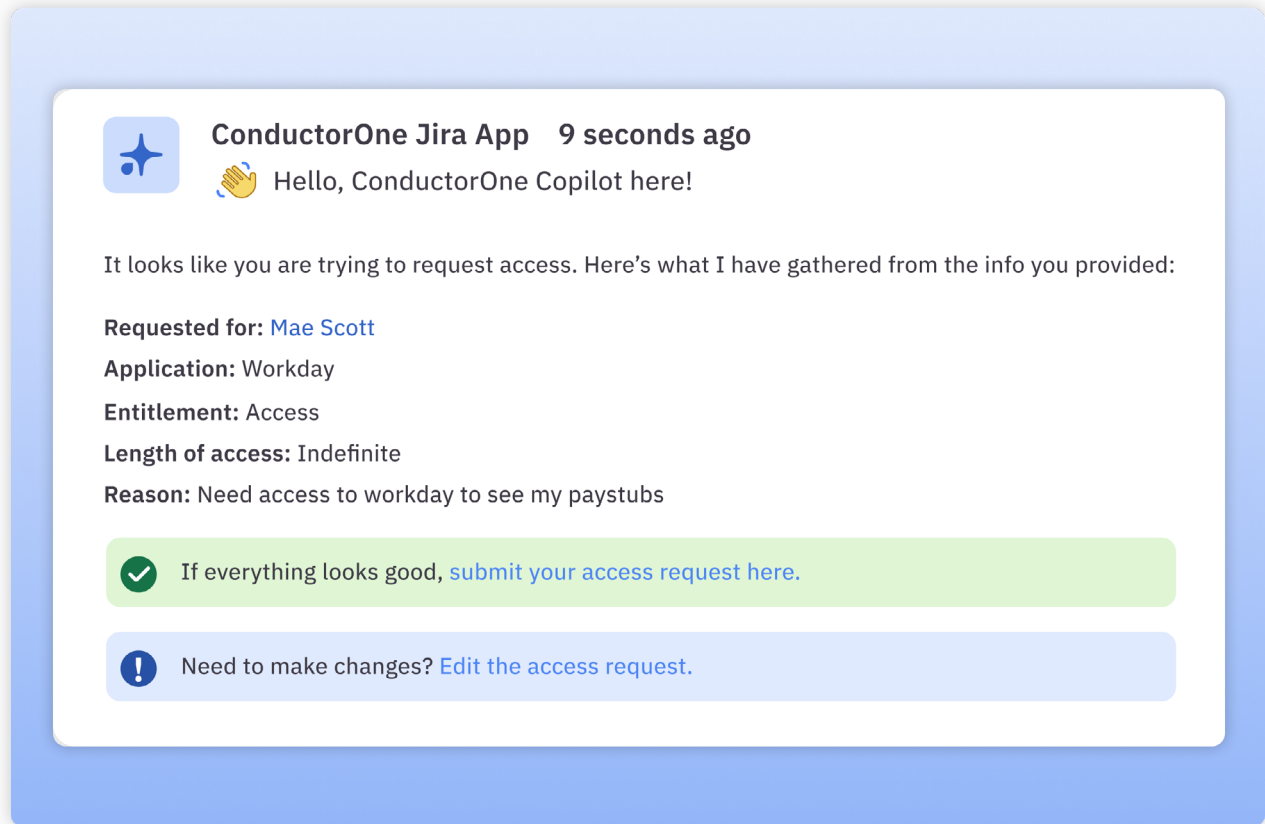
Assign this review to:

Group part of the approval policy



Which group?

AI for Helpdesk Automation

For customers who prefer to use their existing helpdesk system for access requests but want to automate ticket processing on the backend, ConductorOne's AI-powered Copilot can automate the processing of helpdesk request tickets, from reading to approving and provisioning.



ConductorOne Jira App 9 seconds ago

  Hello, ConductorOne Copilot here!

It looks like you are trying to request access. Here's what I have gathered from the info you provided:


Requested for: [Mae Scott](#)


Application: Workday

Entitlement: Access

Length of access: Indefinite

Reason: Need access to workday to see my paystubs

 If everything looks good, [submit your access request here.](#)

 Need to make changes? [Edit the access request.](#)

Developer-Friendly Configuration

ConductorOne supports configuration via Terraform, access requests through its command-line tool (Cone), and extensive automation capabilities through the ConductorOne API. These features make it highly appealing to technical teams that value efficiency and integration flexibility in their workflows.

```
logan in 🌐 logan in ~ via js v19.6.0 took 3s
at 22:15:19 ❌ > cone get lpass-okta --wait -j "Need access for a project"
Ticket URL: https://logan.conductor.one/task/10032
Id | Display Name | State | Processing
10032 | Grant Logan Saso 1Password Business App Access | Closed | Done

SUCCESS Entitlement granted successfully

logan in 🌐 logan in ~ via js v19.6.0 took 3s
at 22:15:32 > cone drop lpass-okta --wait -j "Project completed"
Ticket URL: https://logan.conductor.one/task/10033
Id | Display Name | State | Processing
10032 | Revoke Logan Saso 1Password Business App Access | Closed | Done
```

 [Learn more about access management →](#)

Why Do Customers Choose ConductorOne?

- **Automation-Centric Approach.** ConductorOne prioritizes automation to streamline identity governance and administration processes. This reduces manual workload, speeds up response times, and minimizes the potential for human error. By automating routine tasks like provisioning, deprovisioning, and access reviews, organizations can ensure compliance and maintain tight security with less effort.
- **User-Friendly Interface.** The platform offers a clean, intuitive interface that simplifies complex IAM tasks. It is designed to be user-friendly, allowing both technical and non-technical users to manage access controls effectively. This accessibility enhances user adoption rates and ensures that security policies are consistently applied across the organization.
- **Time to value.** ConductorOne is designed to meet companies where they are and integrate with their existing technology stack quickly, providing security and compliance benefits in a matter of days to weeks. The platform provides a wide range of out-of-the-box connectors for cloud and on-prem apps and infrastructure as well as an open-source connector SDK called [Baton](#) that allows customers to build custom connections to homegrown and private systems.
- **Scalability for Growing Needs.** Whether you're expanding your team or your tech stack, ConductorOne grows with you. It's designed to handle increasing numbers of users and more sophisticated access structures without a drop in performance. Plus, its compatibility with a broad range of applications means it can integrate smoothly into virtually any IT environment.
- **Exceptional Support and Community.** When you choose ConductorOne, you're not just getting a software solution; you're also gaining access to a supportive community and dedicated customer service. This ensures that any issues you encounter are addressed promptly and that you can maximize the benefits of your IAM system.



Case Study

→ [How System1 manages disparate systems after M&A activity and streamlined SOX audits.](#)

CHALLENGES

- ✗ Difficult to manage users, privileges, and roles across multiple systems after M&A activity
- ✗ Slow and time-intensive process to complete user access reviews for SOX compliance
- ✗ Manual effort to collect and validate information for audits

RESULTS

- ✓ Three weeks to integrate with critical in-scope applications like AWS and Okta and launch their first privileged access review campaign
- ✓ Completed SOX audits with significantly less effort with ConductorOne
- ✓ Single pane view into users, roles, and privileges throughout their systems



“With ConductorOne, we're able to have a single pane of glass to look at our systems — and manage users, roles, and access to those systems — which is a huge win for us.”

Jack Chen,
Director of Information Technology, SYSTEM

2. Zluri


Zluri is a comprehensive SaaS management platform that helps organizations optimize their software subscriptions and manage end-to-end software lifecycle from procurement to renewal. It is designed to give IT teams visibility and control over their software stack by providing detailed insights into software usage, spending, and compliance.

The platform offers the ability to automatically discover and inventory all the SaaS applications used across the organization, even those adopted without IT's knowledge. This discovery process aids in identifying redundant apps and underutilized licenses, facilitating cost optimization. Additionally, Zluri offers robust security features, including compliance tracking, [data risk management](#) and assessment, which help ensure that the organization's SaaS environment aligns with industry standards and regulations.

Zluri also simplifies the management of SaaS contracts and vendor relationships. With features like automated renewal reminders and spending analytics, organizations can avoid unnecessary auto-renewals and negotiate contracts more effectively.

Top Features

- **Application Discovery and Management.** With Zluri, organizations can automatically discover all the applications in use across their network. This feature includes management capabilities that allow for the monitoring of software usage, compliance status, and optimization of software spend.
- **One-Click Provisioning and Deprovisioning.** This feature allows IT administrators to instantly grant or revoke access to applications with a single click. It is particularly useful for managing access rights efficiently and securely, minimizing the risk of unauthorized access.
- **Spend Optimization.** Zluri offers advanced spend analysis tools that evaluate historical data and current usage patterns to identify cost-saving opportunities. This includes recommendations for eliminating redundant subscriptions and renegotiating contracts based on actual usage statistics, potentially saving companies significant amounts of money.
- **License Management.** This feature enables organizations to manage their software licenses effectively. Zluri tracks expiration dates, renewal terms, and license utilization. It alerts administrators about over or underutilization, helping to avoid compliance issues and ensuring that investments in software are fully leveraged.
- **Compliance Tracking.** The platform supports compliance with various regulatory standards by continuously monitoring software usage and ensuring that all SaaS applications adhere to specific industry regulations and company policies. It generates compliance reports that can be used for audits, thereby simplifying the compliance management process.

 **ConductorOne Advantage** → ConductorOne offers better integration capabilities that allow it to seamlessly connect with a broader range of software and platforms, offering more flexibility and scalability for growing businesses.

3. Zilla Security

Zilla Security is a specialized security management platform that centralizes control over cloud-based environments and SaaS applications, enabling enterprises to safeguard their digital assets.


It offers a comprehensive suite of tools that makes it easy to detect, analyze, and manage security risks associated with extensive SaaS usage. It provides a granular overview of user activities and application interactions, helping IT security teams to preemptively identify potential security breaches before they materialize.

In addition, Zilla Security's infrastructure is built on robust cloud security protocols, utilizing advanced encryption methods to protect data both in transit and at rest. The platform integrates seamlessly with leading cloud providers and employs end-to-end encryption standards such as AES-256 to secure sensitive data.

In terms of user authentication, Zilla Security uses multi-factor authentication (MFA) systems, enhancing security by requiring multiple forms of verification. It also supports a range of SSO options, which simplifies the user access process while maintaining high security standards.

Top Features

- **SaaS Security Posture Management (SSPM).** Provides tools to continuously assess and manage the security risks associated with SaaS applications. This includes identifying misconfigurations, excessive permissions, and compliance deviations in real-time.
- **Compliance Tracking Dashboard.** Provides a comprehensive view of an organization's compliance status with various regulatory requirements. It automatically aggregates data and presents it in an easy-to-understand format to track progress and identify areas needing attention.
- **Zilla Universal Sync (ZUS).** Streamlines application integration, especially those without security APIs. It uses robotic automation to easily gather user accounts and permissions information, making the process quick and straightforward with just a few clicks.
- **Zilla PO Box.** Optimized for secure interactions with on-premises systems, this containerized solution supports various connection methods including APIs, file imports, SQL queries, and robotic automation, ensuring comprehensive connectivity.
- **Closed-Loop ITSM Ticketing.** Zilla enhances ITSM systems by tracking and documenting all change requests related to user access and account security. It actively identifies and flags any unresolved issues or access revocations, ensuring thorough follow-up until issues are fully resolved.
- **Extensive Integration Ecosystem.** Zilla offers a powerful platform with over 1000 ready-to-use integrations, facilitating secure and straightforward connections with any application. It supports multiple integration methods like REST API, Zilla Universal Sync, file imports, and Zilla PO Box, making it compatible with both API-supported and non-API applications.

 **ConductorOne Advantage** → ConductorOne's real-time analytics provide deeper insights into access patterns and potential security risks, allowing organizations to manage their security posture more effectively.

4. SailPoint


SailPoint is an enterprise identity governance platform that delivers powerful solutions for comprehensive visibility into an organization's access management. It covers who is doing what, who should have access, and how that access is being used.

SailPoint is designed to handle complex access environments across a wide range of on-premises and cloud-based systems, ensuring that the right individuals have the right access to the right resources at the right times for the right reasons, thereby enforcing policy compliance.

Its AI-driven identity analytics feature provides organizations with actionable insights into access risks and anomalies. This enables effective management of potential security breaches and compliance issues. SailPoint also streamlines access certifications, role management, and audit reporting, which are critical for maintaining compliance with regulations such as GDPR, [HIPAA](#), and [SOX](#).

Top Features

- **Access Modeling.** Allows organizations to simulate and model access changes within SailPoint before they are applied. This helps in understanding the implications of access changes, ensuring they align with security and compliance requirements.
- **File Access Manager.** Protects sensitive unstructured data stored across files and cloud storage. It automatically discovers where sensitive data resides and who has access to it, providing visibility and control over this data.
- **IdentityIQ.** This is SailPoint's flagship identity governance platform that integrates with existing IT infrastructures to manage digital identities effectively. It provides comprehensive governance capabilities across all users, applications, and data, ensuring that access rights are granted according to policies and are compliant with regulations.
- **Automated Access Recommendations.** Streamlines the often lengthy certification processes, enabling quicker and more informed access decisions. Utilizing advanced algorithms, it provides automated recommendations derived from peer group analyses, identity attributes, and historical access activities, enhancing decision-making accuracy.
- **Password Manager.** simplifies password management across various platforms. It reduces password-related helpdesk calls by allowing users to reset their passwords autonomously through a secure, web-based portal.
- **Role Management.** Includes role-based access control (RBAC) capabilities, which help to streamline the assignment of access rights by grouping permissions into roles based on job functions.

 **ConductorOne Advantage** → ConductorOne's real-time analytics provide deeper insights into access patterns and potential security risks, allowing organizations to manage their security posture more effectively.

5. Okta Workforce Identity Cloud

Okta Workforce Identity Cloud is a cloud identity and access management solution that secures and streamlines user access across any application or device.


As a cloud-based platform, it enables organizations to implement strong security measures without the overhead of traditional on-premises solutions. Okta focuses on enhancing user productivity and security through a seamless and secure login experience across multiple platforms.

A major Okta feature is its Universal Directory, which offers a centralized system for managing and syncing user data across all applications and services within an organization. This integration capability extends to thousands of pre-built integrations for popular applications and IT systems, making Okta highly adaptable to multiple IT environments.

Furthermore, Okta provides robust policy frameworks and detailed reporting tools that help organizations meet compliance standards and audit requirements. This makes Okta Workforce Identity Cloud a powerful tool for organizations needing a flexible, scalable, and secure identity management solution.

Top Features

- **Adaptive Multi-Factor Authentication (MFA)**. Okta provides robust security with adaptive MFA that evaluates the risk level of each access request based on factors such as location, device, and user behavior.
- **Lifecycle Management**. Okta automates the entire lifecycle of user identities with efficient provisioning and deprovisioning processes. It integrates with HR systems to ensure that changes in employment status are reflected promptly across all applications.
- **API Access Management**. Okta secures APIs by ensuring that only authorized users and services can access them, utilizing OAuth and OpenID Connect protocols to protect sensitive data and transactions.
- **Advanced Server Access (ASA)**. Provides secure, identity-led access to infrastructure resources such as servers and databases both on-premises and in the cloud. It offers a Zero Trust approach to server access, enforcing least privilege and providing session visibility and control.
- **Access Gateway**. Secures simple, and integrated access to on-premises applications without changing how those applications are configured, using industry standards such as SAML and SWA.
- **Okta Single Sign-On (SSO)**. Guarantees users an easy and secure access to all their applications through one login portal. It supports thousands of pre-integrated apps and includes a robust set of integration tools for new or custom applications.

 **ConductorOne Advantage** → ConductorOne can connect to apps and systems outside of a customer's IdP and enables access control to more fine-grained resources.

6. Microsoft Entra ID

Microsoft Entra ID, previously known as Microsoft Azure Active Directory (Azure AD), is an IAM service provided by Microsoft as part of its cloud security offerings.

The platform provides comprehensive tools for identity protection, such as [user and entity behavior analytics \(UEBA\)](#) and automated threat detection, which help prevent identity-based security breaches.


Microsoft Entra ID allows IT administrators to efficiently manage access to applications and resources, customizing it according to specific business requirements. For example, it supports the implementation of multifactor authentication for accessing critical organizational resources.

Additionally, Microsoft Entra ID automates user provisioning between Windows Server AD and various cloud applications, including Microsoft 365, ensuring a secure and seamless integration.

For businesses heavily invested in the Microsoft ecosystem, Microsoft Entra ID offers a particularly compelling solution due to its native integration, extensive scalability, and robust security features.

Top Features

- **Secure Hybrid Access.** This feature bridges on-premises and cloud environments, facilitating secure access to applications regardless of where they are hosted. It leverages Azure AD Application Proxy and various authentication methods to ensure that users can safely connect to enterprise applications from any location.
- **Conditional Access.** This is a policy-based engine within Microsoft Entra that allows organizations to enforce automated access-control decisions based on conditions for accessing network and cloud-based applications. It integrates seamlessly with other Microsoft services, leveraging real-time data analytics to enhance security without compromising user experience.
- **Passwordless Authentication.** Supports biometrics, hardware tokens, or Windows Hello, to simplify and strengthen user access security. This method eliminates the need for passwords, reducing the risk associated with their theft or misuse.
- **Privileged Identity Management (PIM).** This feature helps control, manage, and monitor access to critical resources within an organization. PIM includes just-in-time privileged access, which reduces risks by granting necessary permissions temporarily.
- **Cross-Platform Compatibility.** Microsoft Entra ID is designed to work seamlessly across both Microsoft and non-Microsoft environments. It supports integration with various cloud and on-premises applications.

 **ConductorOne Advantage** → ConductorOne offers a more streamlined approach compared to Microsoft Entra ID, focusing on simplifying the user experience without sacrificing security features.

7. Ping Identity

Ping Identity is an advanced IAM tool designed to improve security and user experience across digital enterprises. It focuses on providing seamless, secure access to cloud, mobile, SaaS, and on-premises applications while protecting sensitive data from breaches.


Ping Identity is flexible, making it easily adaptable to complex IT environments. It also supports multiple authentication protocols and standards, including OAuth, OpenID Connect, and SAML.

The platform uses AI and machine learning to intelligently manage access and detect potential security threats in real time. It also includes comprehensive API security features that protect both internal and external APIs from common vulnerabilities.

Additionally, Ping Identity offers extensive customization options, enabling organizations to adjust the user experience and security controls to suit specific business needs and comply with regulatory requirements.

Top Features

- **PingOne Risk Management.** Utilizes analytics to assess the risk associated with user access requests, then determines the likelihood of a request being fraudulent and applies appropriate security measures to mitigate risks.
- **PingIntelligence for APIs.** This feature leverages AI and machine learning to protect APIs by detecting and mitigating threats in real-time. It ensures that only authenticated users and secure devices can access sensitive API functions.
- **PingFederate.** This is an identity federation and access management solution that simplifies user authentication and single sign-on (SSO) across different organizations and applications. It supports standards such as SAML, WS-Federation, and OAuth, facilitating secure, cross-domain interactions.
- **PingDirectory.** This is a highly scalable and customizable directory server that provides a secure data store for user and device profiles. It is designed to handle large volumes of identity data and complex query operations.
- **PingAccess.** Allows for fine-grained access control to applications and APIs, whether they are hosted on-premises or in the cloud. It works seamlessly with PingOne and other identity management systems to enforce policies that limit resource access based on user roles, attributes, and other contextual factors.
- **PingID.** This offers robust multi-factor authentication to ensure secure access to applications and services. It supports various authentication methods including biometrics, SMS, email, and push notifications. It also adapts the authentication strength based on the user's location, device, and network, providing a balance between security and user experience.

 **ConductorOne Advantage** → ConductorOne offers self-service capabilities, allowing end-users to manage their credentials and access rights more efficiently, which reduces IT overhead and enhances overall user satisfaction.

8. Oracle Access Management


Oracle Access Management (OAM) is a component of the Oracle Fusion Middleware Identity and Access Management Suite. This suite includes Oracle Access Manager, Oracle Advanced Authentication (OAA), Oracle RADIUS Agent (ORA), and extended support for the legacy software Enterprise Single Sign-On (ESSO).

Together, these solutions offer fully integrated services that enhance traditional access management capabilities. They extend security from on-premises systems to the cloud in a scalable manner, making it a robust choice for modern IT environments.

Additionally, Oracle IAM features predictive analytics tools that use machine learning to identify and address potential security threats by analyzing user behavior patterns.

Top Features

- **OAM Stateless Mid-tier.** This feature enables database state persistence with a stateless mid-tier, simplifying upgrades and cloud migrations. It supports new use cases like linking sessions across web, API, and device access, and consolidates state across Single Sign-On (SSO), federation, and OAuth.
- **Oracle Mobile Authenticator (OMA).** OMA now supports an enhanced enrollment process for adding accounts to the OMA app. Organizations can utilize the App Protection feature to secure the OMA app with biometric identifiers like Touch ID for iOS and Fingerprint for Android.
- **Oracle Advanced Authentication (OAA).** OAA enhances Multi-Factor Authentication (MFA) with modern, passwordless factors such as FIDO2 and YubiKey. It integrates with the new microservice, Oracle RADIUS Agent (ORA), enhancing protection for Oracle databases, VPNs, and SSH sessions with a modern MFA user experience.
- **OAM Snapshot Tool.** This tool aids administrators in managing, migrating, and updating OAM deployments uniformly across different infrastructures, leveraging Oracle Database backup and cloning solutions.
- **Multi Data Center Lifecycle Simplification.** OAM streamlines the setup and management of multi-data center (MDC) topologies, using new REST-based APIs for administrative and diagnostic purposes to reduce setup complexity. OAuth artifacts like Identity Domains and Clients are synchronized across data centers.
- **OAM Container Image.** This facilitates the deployment of OAM on-premises and in the cloud using Kubernetes. This allows for automated deployments and upgrades, auto-scaling, and portability across multi-cloud and on-premises environments.

 **ConductorOne Advantage** → ConductorOne offers a more lightweight and flexible solution compared to Oracle Access Management. This makes it ideal for businesses that require quick deployment and easy scalability without the complexity often associated with large-scale IAM systems.

9. OneLogin

OneLogin is a Unified Access Management (UAM) platform that centralizes all your organization's access, both on-premises and in the cloud. It provides comprehensive control, management, and security for your data, devices, and users.


The platform streamlines various administrative tasks, including application rollout, new employee onboarding, and de-provisioning, while reducing access-related helpdesk requests by over 50% through a self-service password reset feature.

It ensures real-time synchronization between the OneLogin Cloud Directory and multiple Active Directories, eliminating the manual maintenance of these systems. Users benefit from one-click access to all their applications via a secure portal, accessible from anywhere at any time.

Additionally, OneLogin extends single sign-on (SSO) capabilities to MacOS and Windows devices and integrates legacy applications on-premises or hosted remotely, thus enhancing both usability and security.

Top Features

- **App Catalog.** OneLogin's catalog boasts over 5,000 pre-integrated applications, simplifying the implementation of single sign-on (SSO) and user provisioning for enterprise apps.
- **Adaptive Authentication.** Utilizes machine learning to conduct dynamic risk assessments, identifying high-risk login attempts and prompting multi-factor authentication (MFA). Risk scores are generated based on factors such as network reputation, geographic location, device fingerprinting, and time anomalies.
- **One Click On- and Off-Boarding.** Automates onboarding and offboarding processes by importing entitlement definitions from each app and establishing flexible rules for assigning user entitlements. It features real-time synchronization with Active Directory, ensuring that any changes, such as disabling a user, are reflected in target applications within seconds.
- **Unified Endpoint Management.** Integrates your laptop or desktop with the OneLogin Cloud Directory, creating a secure profile on your machine accessible only with OneLogin credentials. This setup allows a single login to your operating system to automatically log you into all linked applications, eliminating the need for additional browser logins.
- **Mobile Identity.** Provides secure access to all cloud and enterprise apps, running web apps inside the mobile platform as fully functional web applications without leaving any data trail.
- **VigilanceAI.** VigilanceAI, OneLogin's proprietary machine learning engine, analyzes extensive data from both internal and external sources to establish individual user behavior profiles. This enables it to detect and alert on behavioral anomalies in real-time, offering advanced threat defense.

 **ConductorOne Advantage** → ConductorOne's advanced analytics and reporting capabilities provide deeper insights into access behaviors and potential vulnerabilities.

10. IBM Security Verify


IBM Security Verify is a robust IAM solution that empowers security teams to implement risk-based access policies, facilitating frictionless user authentications across web, mobile, and cloud applications, as well as APIs.

Leveraging standard protocols, it offers Identity-as-a-Service, helping organizations to enhance security and modernize digital experiences for both internal workforce and external consumers.

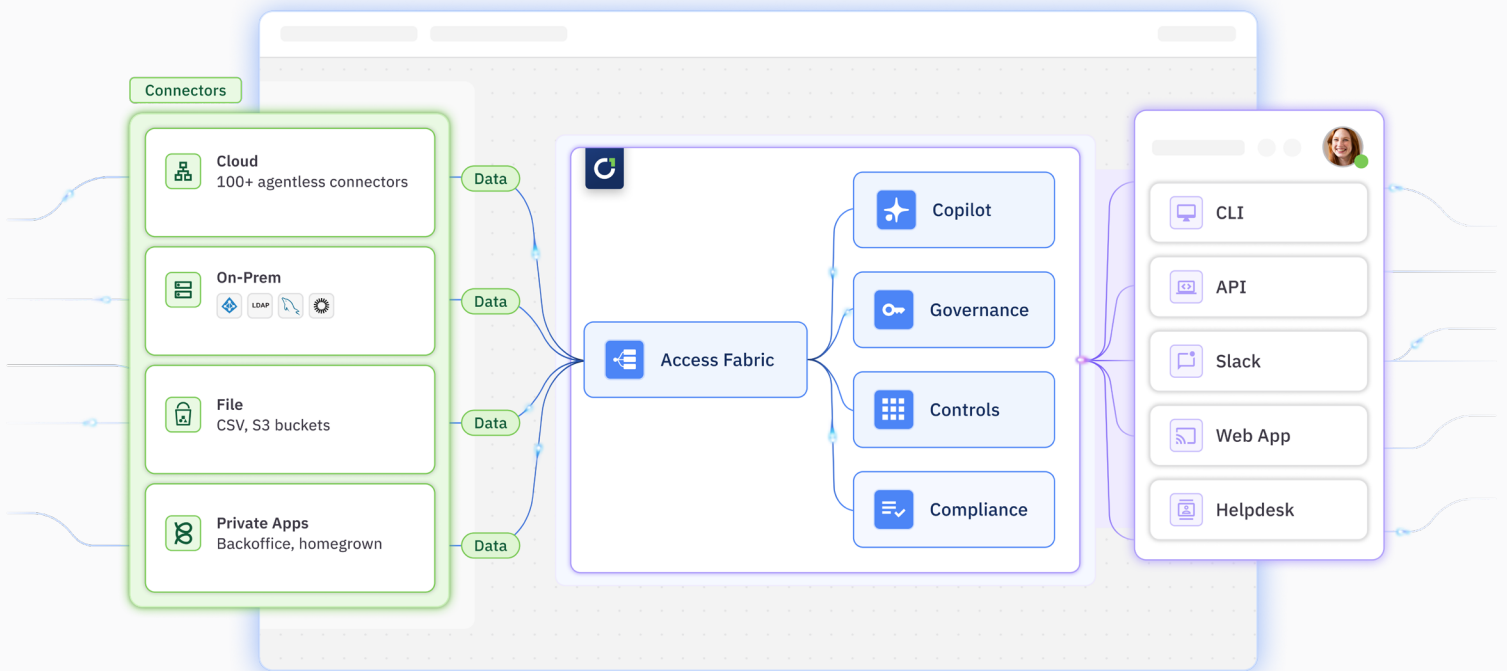
Additionally, IBM Security Verify ensures seamless, secure access to applications and complements native AWS services, streamlining integration and enhancing overall security posture.

Top Features

- **Centralized Credential Vault.** Encrypts and centralizes all privileged credentials within a secure vault, providing authorized access while enforcing strict security controls.
- **Comprehensive Account Identification.** Automatically identifies all types of privileged accounts, including service, application, administrator, and root accounts, ensuring complete visibility and management of access rights.
- **Automated Password Management.** Automates the process of password changes, enforces complex password creation, and systematically rotates credentials to secure accounts against unauthorized access.
- **Managed Access and Monitoring.** Controls and monitors user sessions through session launching, use of proxies, active monitoring, and recording, enhancing both security and accountability.
- **Single Agent Monitoring.** Utilizes a single agent to discover and monitor applications operated with administrative privileges on both domain and non-domain machines, streamlining management and enhancing security coverage.

 **ConductorOne Advantage** → ConductorOne offers enhanced automation features that streamline identity governance and administrative tasks. This results in significant time savings and reduced human errors.

Centralize Control and Simplify User Access Management with ConductorOne



Imagine managing all your identity and access controls from one powerful platform – ConductorOne makes this a reality.

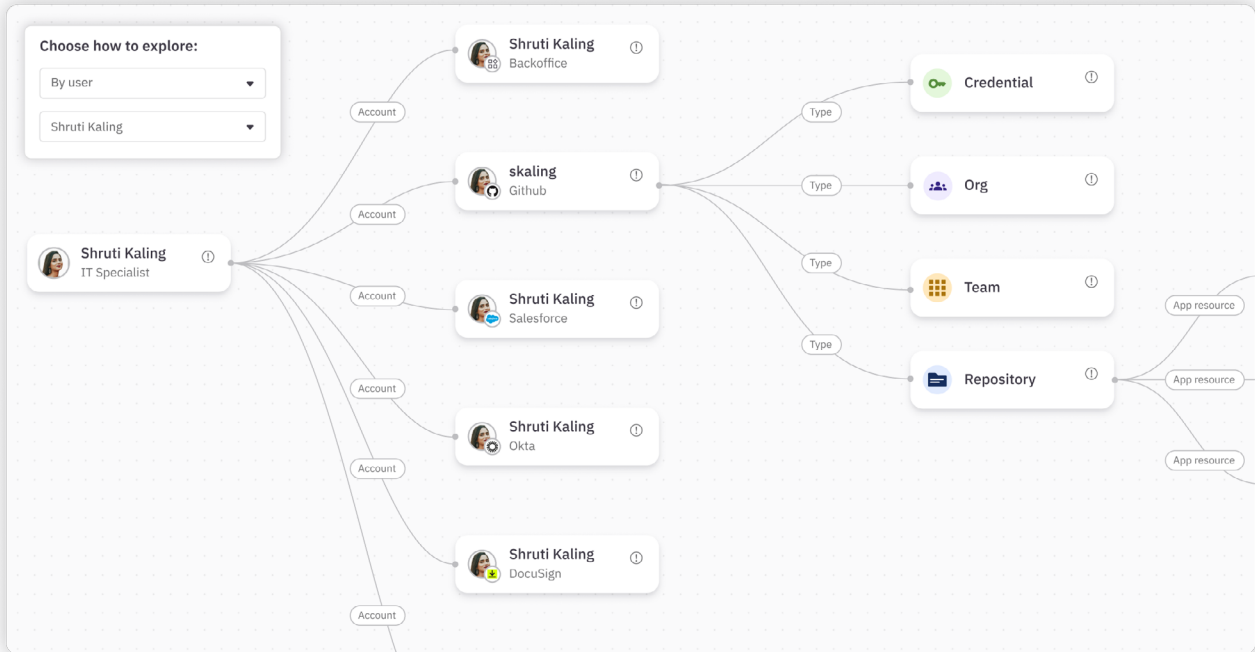
By centralizing control, ConductorOne simplifies the complexity of managing multiple systems and significantly cuts down the chances of errors. You gain clear oversight over user activities and permissions, ensuring that your organization's data is always protected and compliance is maintained.

Explore Data



Orphaned accounts	24	Inactive users	143	Standing privilege	61
Updated 1 min ago					
AWS	8	Okta	54	Salesforce	54
Slack	4	Slack	23	Slack	23
GitHub	3	GitHub	12	GitHub	12
Okta	3	AWS	7	AWS	7
Tailscale	2	Tailscale	7	Tailscale	7
View all					

High-risk users	4	High-risk roles (ongoing)	37	High-risk roles (temporary)	37
Updated 1 min ago					
Anita Miller anitamiller@amitysoft.io	5 grants	Super Admin	9	User Mgmt Admin	12



ConductorOne streamlines your daily operations by automating routine tasks such as user provisioning and deprovisioning. This automation reduces the need for manual oversight, drastically lowering the risk of security breaches that can occur due to human error.

In addition, ConductorOne ensures that access rights are always aligned with the latest policies and swiftly adjusts to changes in user roles or business requirements.

By choosing ConductorOne, you move toward a more controlled and simplified access management system that puts your needs—and security—first.

Talk to our team.

Or take a self-guided tour
to learn more!

Try ConductorOne now

[Get a demo](#)