ConductorOne

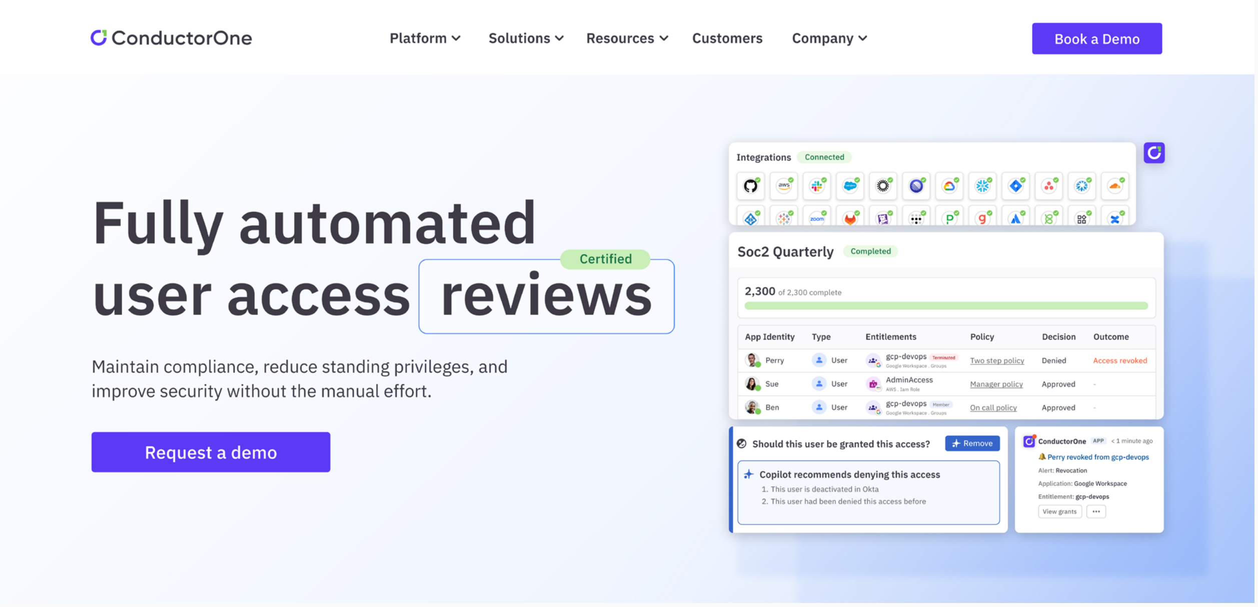
The 9 Best User Access Review (UAR) Software for Cybersecurity in 2024

User access reviews (UARs) are periodic audits to ensure that users have appropriate access rights based on their current roles and responsibilities. These reviews are essential for preventing unauthorized access and maintaining compliance with various regulatory standards such as SOX, HIPAA, and GDPR.

The 9 Best User Access Review Tools Right Now

1. ConductorOne
2. SailPoint IdentityIQ
3. Microsoft Entra
4. CyberArk Identity
5. Ping Identity
6. ManageEngine ADAudit Plus
7. Lumos
8. LogicManager
9. SecurEnds

1. ConductorOne — Access Reviews Made Easier



Fully automated user access reviews

Maintain compliance, reduce standing privileges, and improve security without the manual effort.

Soc2 Quarterly Completed

2,300 of 2,300 complete

App Identity	Type	Entitlements	Policy	Decision	Outcome
Perry	User	gcp-devops Terminated Google Workspace . Groups	Two step policy	Denied	Access revoked
Sue	User	AdminAccess AWS . Iam Role	Manager policy	Approved	-
Ben	User	gcp-devops Member Google Workspace . Groups	On call policy	Approved	-

Should this user be granted this access? Remove

Copilot recommends denying this access

1. This user is deactivated in Okta
2. This user had been denied this access before

ConductorOne APP < 1 minute ago

Perry revoked from gcp-devops

Alert: Revocation

Application: Google Workspace

Entitlement: gcp-devops

View grants ···

ConductorOne is an access control platform designed to manage and secure user access across all of an organization's applications and infrastructure. It centralizes the control of identity and access management, offering automated solutions to streamline security protocols and ensure compliance in modern IT environments.

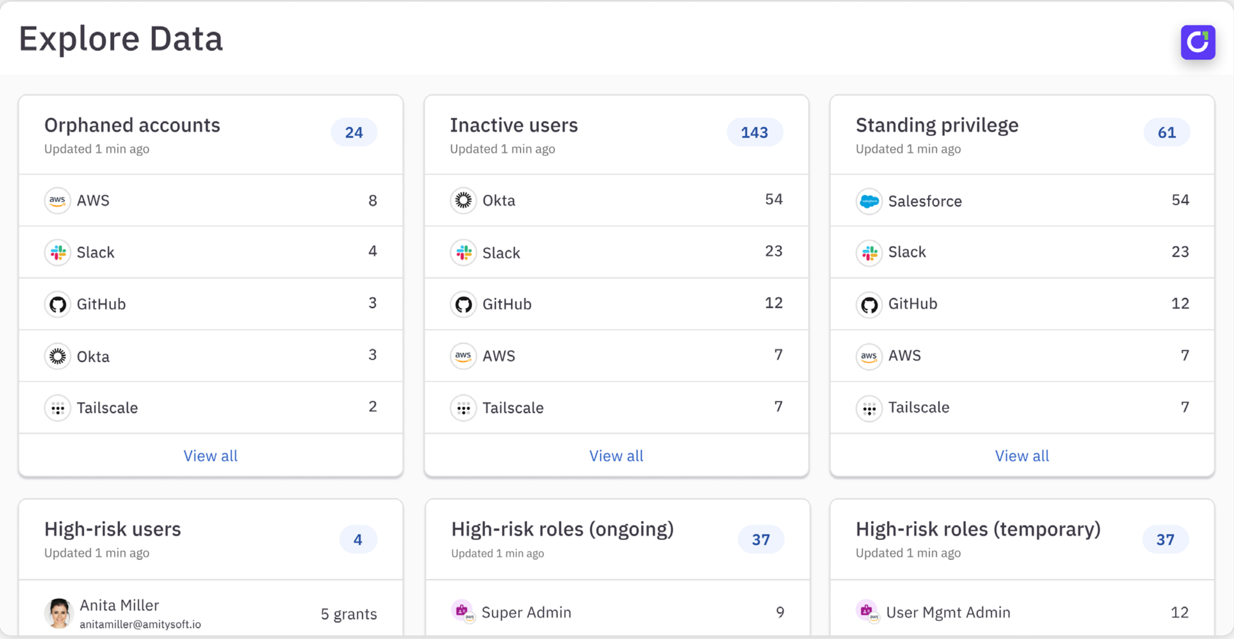
The platform supports agentless connectors that integrate seamlessly with various systems, enhancing visibility and control without requiring extensive manual setup. The extensible platform supports the use of modern tools like Terraform and webhooks, allowing IT and security teams to configure as code and create custom workflows, thus providing a scalable and efficient solution for handling access rights across complex environments.

Watch → Access Review Product Overview - ConductorOne

Key Features of ConductorOne's User Access Reviews

Access Fabric — Complete Identity Visibility

ConductorOne's access fabric is the foundational data layer underpinning the platform's powerful access control and governance capabilities. It enables visibility and control over user access across an organization's applications and infrastructure by creating a central source of truth for identity and access management, allowing IT and security teams to efficiently monitor and manage access rights.



Explore Data

Orphaned accounts Updated 1 min ago	24
AWS	8
Slack	4
GitHub	3
Okta	3
Tailscale	2
View all	

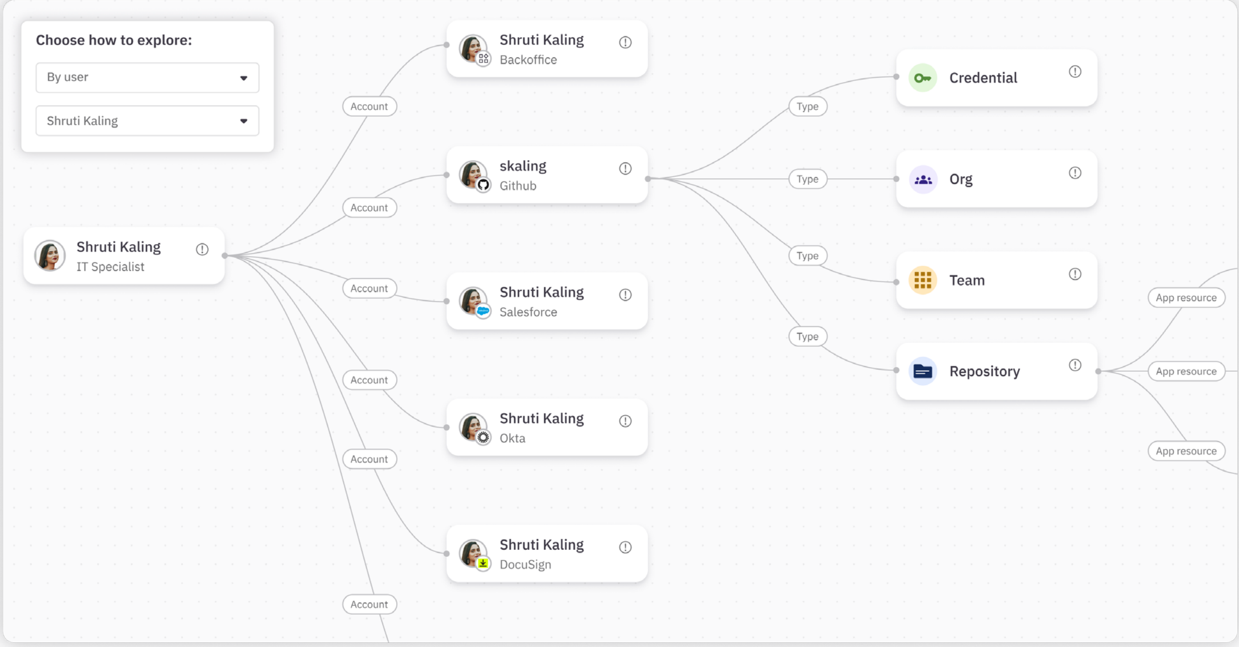
Inactive users Updated 1 min ago	143
Okta	54
Slack	23
GitHub	12
AWS	7
Tailscale	7
View all	

Standing privilege Updated 1 min ago	61
Salesforce	54
Slack	23
GitHub	12
AWS	7
Tailscale	7
View all	

High-risk users Updated 1 min ago	4
Anita Miller anitamiller@amitysoft.io	5 grants

High-risk roles (ongoing) Updated 1 min ago	37
Super Admin	9

High-risk roles (temporary) Updated 1 min ago	37
User Mgmt Admin	12



Choose how to explore:

By user

Shruti Kaling

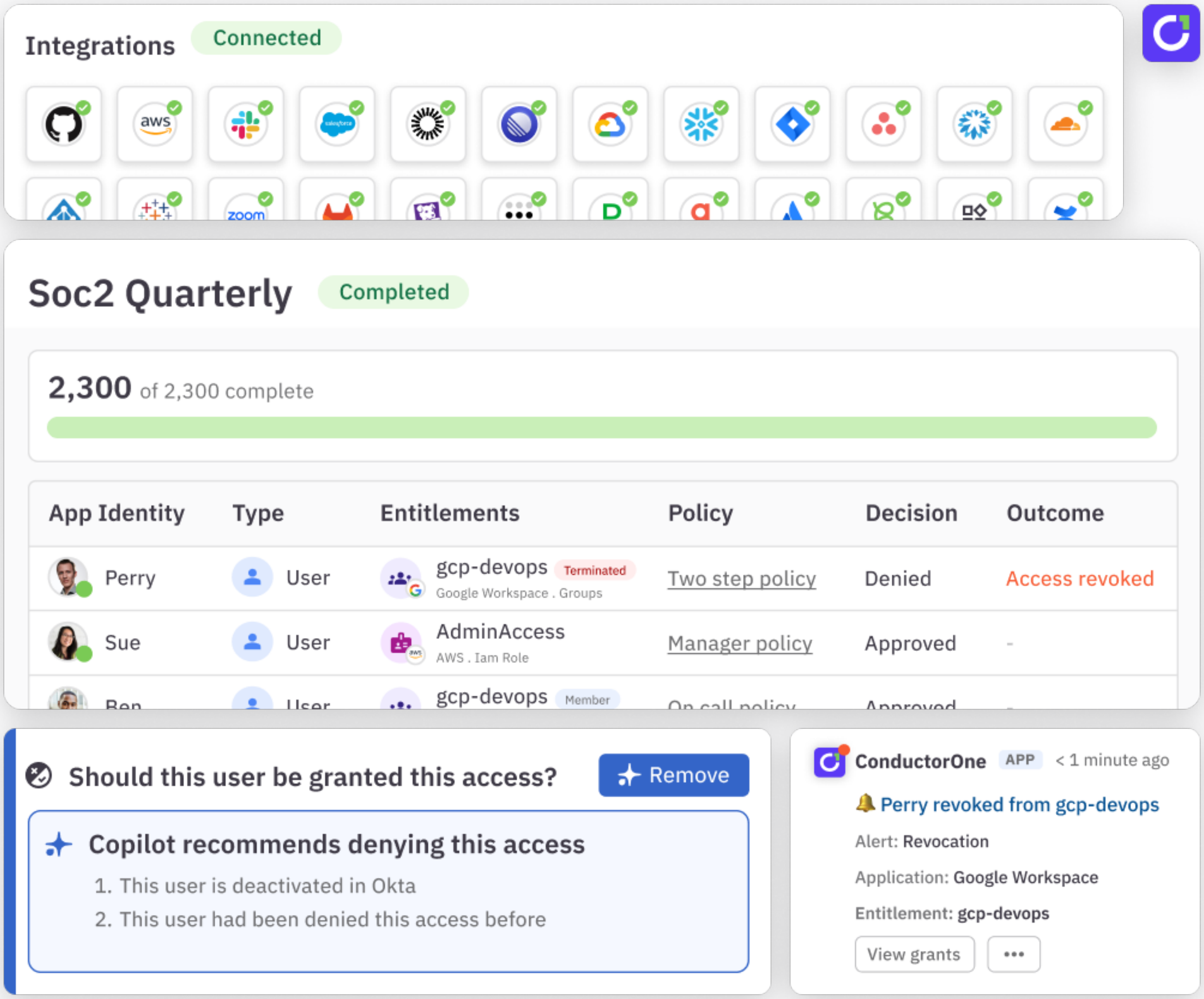
The access fabric integrates data from various sources—including cloud services, on-premise applications, HR systems, and directories—to offer a comprehensive view of all identities and their access privileges.

One of the access fabric's key benefits is its ability to help organizations identify and address access risks such as orphaned accounts, inactive users, and high-risk access privileges. The platform offers powerful search capabilities that enable users to quickly find and rectify these risks, thereby reducing the organization's overall security vulnerability. With ConductorOne, organizations can also proactively detect and remediate separation of duties (SoD) conflicts.

> 💡 **Access fabric** includes an easy-to-use visualization tool that allows teams to view access paths for any user, application, or resource, which can significantly aid in understanding and managing permissions more effectively. It also provides built-in remediation options that facilitate prompt action to secure at-risk accounts or adjust inappropriate access rights.

Automated Access Reviews

This product is designed to streamline the process of managing and auditing user access across various systems and applications within an organization.



Soc2 Quarterly

Completed

2,300 of 2,300 complete

App Identity	Type	Entitlements	Policy	Decision	Outcome
Perry	User	gcp-devops Terminated Google Workspace . Groups	Two step policy	Denied	Access revoked
Sue	User	AdminAccess AWS . Iam Role	Manager policy	Approved	-
Ben	User	gcp-devops Member	On call policy	Approved	-

Should this user be granted this access? Remove

Copilot recommends denying this access

1. This user is deactivated in Okta
2. This user had been denied this access before

ConductorOne APP < 1 minute ago

🔔 Perry revoked from gcp-devops

Alert: Revocation

Application: Google Workspace

Entitlement: gcp-devops

View grants •••

The system automates the entire access review process, from scoping and scheduling reviews to notifying reviewers via integrated communication tools like email or Slack. This automation helps eliminate the traditional reliance on spreadsheets and manual tracking, thereby speeding up the review process and reducing errors.

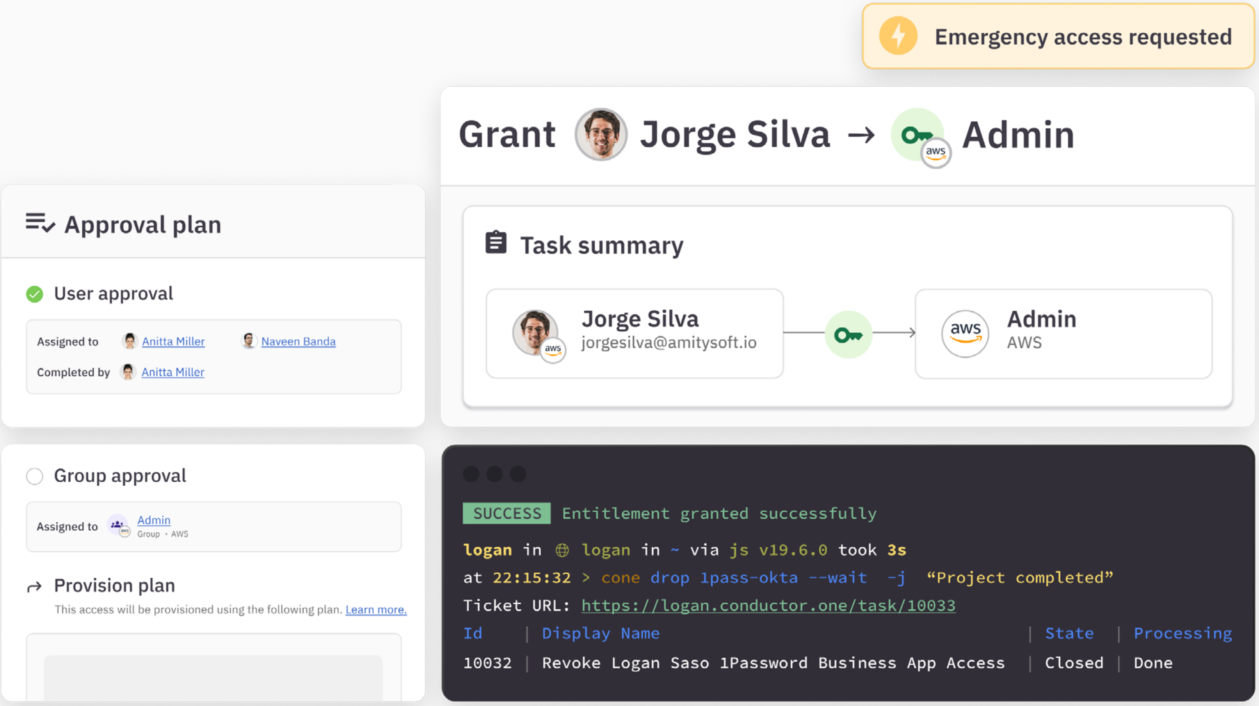
> 💡 ConductorOne supports multi-step reviewer policies and provides automation features like auto-approvals and zero-touch deprovisioning for offboarding.

Self-Service Access Requests

The platform also allows users to request access to applications, groups, roles, or permissions through an intuitive self-service app catalog that can be accessed via Slack, CLI, or web app.
Requests are automatically routed to the appropriate approvers with all the necessary context and analysis, which helps approvers make informed decisions quickly. Upon approval, access can be granted immediately through automated provisioning processes. This can be done directly to the application or via identity providers (IdPs), using standards like SCIM, or through manual workflows if needed.

Just-in-Time Access

JIT access facilitates immediate and temporary access provisioning to resources, which is then automatically revoked after a predetermined period or upon completion of a task. This helps in maintaining tight security controls and reducing standing privileges.



Task summary

Jorge Silva
jorgesilva@amitysoft.io

Admin
AWS

Approval plan

✓ User approval

Assigned to Anitta Miller Naveen Banda
Completed by Anitta Miller

○ Group approval

Assigned to Admin
Group • AWS

Provision plan

This access will be provisioned using the following plan. Learn more.

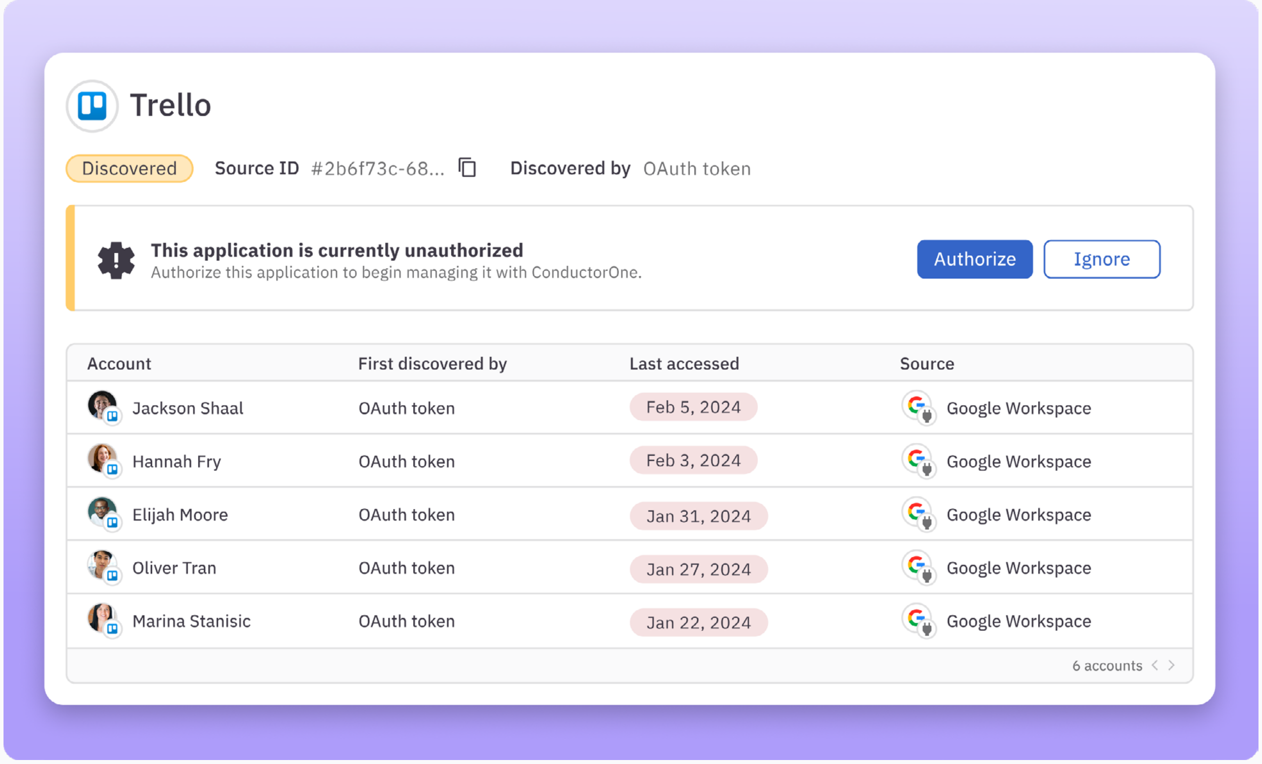
```
SUCCESS Entitlement granted successfully
logan in 🌐 logan in ~ via js v19.6.0 took 3s
at 22:15:32 > cone drop 1pass-okta --wait  -j  “Project completed”
Ticket URL: https://logan.conductor.one/task/10033
Id    | Display Name                           | State  | Processing
10032 | Revoke Logan Saso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

Access request approvals can be configured to follow strict policy-driven workflows, where approvals are granted based on the user’s role, the sensitivity of the accessed resources, and other criteria.

Shadow IT Detection

ConductorOne can detect and manage unauthorized app usage, helping secure environments against potential breaches initiated through unmonitored applications. The platform provides real-time insights into shadow app usage by monitoring who uses these applications and when they are used.

For example, when an employee uses their IdP credentials to log into an unauthorized app, that activity will be logged in ConductorOne. Newly discovered shadow apps will be listed on the shadow apps page, and users can view subsequent employee login activity as it occurs.



Trello

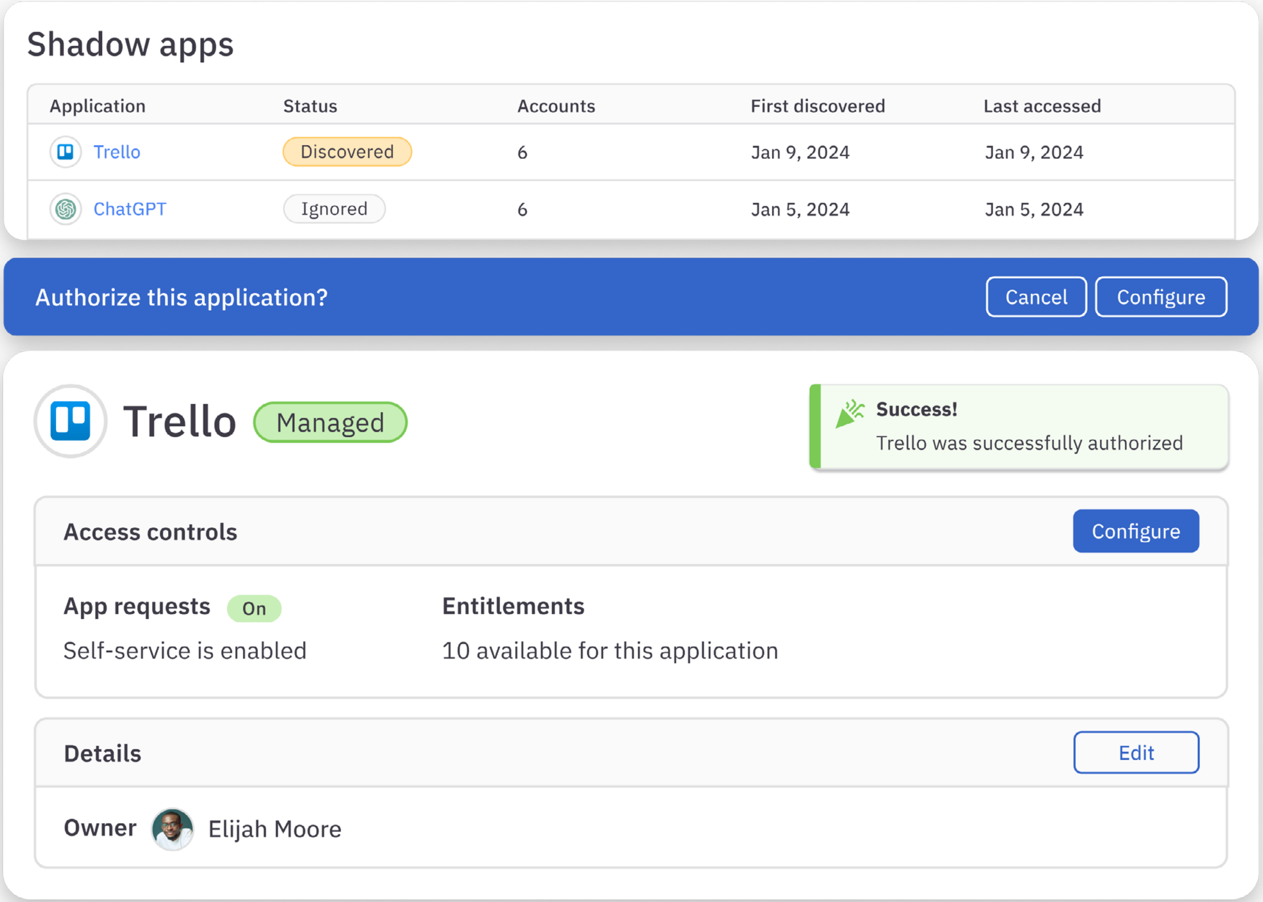
Discovered   **Source ID** #2b6f73c-68...   **Discovered by** OAuth token

This application is currently unauthorized
Authorize this application to begin managing it with ConductorOne.

Account	First discovered by	Last accessed	Source
Jackson Shaal	OAuth token	Feb 5, 2024	Google Workspace
Hannah Fry	OAuth token	Feb 3, 2024	Google Workspace
Elijah Moore	OAuth token	Jan 31, 2024	Google Workspace
Oliver Tran	OAuth token	Jan 27, 2024	Google Workspace
Marina Stanisic	OAuth token	Jan 22, 2024	Google Workspace

6 accounts

Shadow apps can be brought under management in ConductorOne with a few clicks. Once authorized and assigned an owner, the app is added to the list of applications in ConductorOne and can be managed like any other app.



Shadow apps

Application	Status	Accounts	First discovered	Last accessed
Trello	Discovered	6	Jan 9, 2024	Jan 9, 2024
ChatGPT	Ignored	6	Jan 5, 2024	Jan 5, 2024

Authorize this application?

Success!
Trello was successfully authorized

Access controls

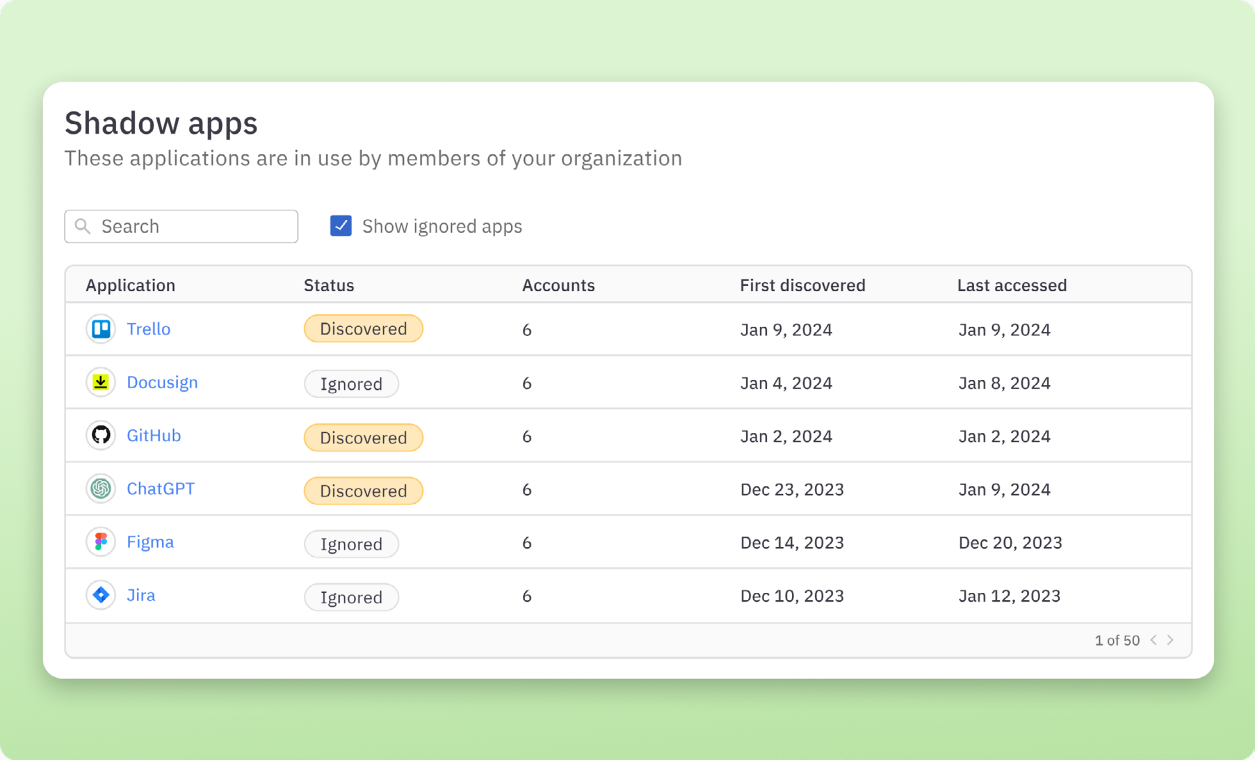
App requests On
Self-service is enabled

Entitlements
10 available for this application

Details

Owner Elijah Moore

Shadow apps that aren’t of current concern can also be ignored. Ignoring a shadow app removes it from the active list of tracked shadow apps, but ConductorOne will continue to log the app’s usage activity, and the app can be un-ignored and brought under management at any time.

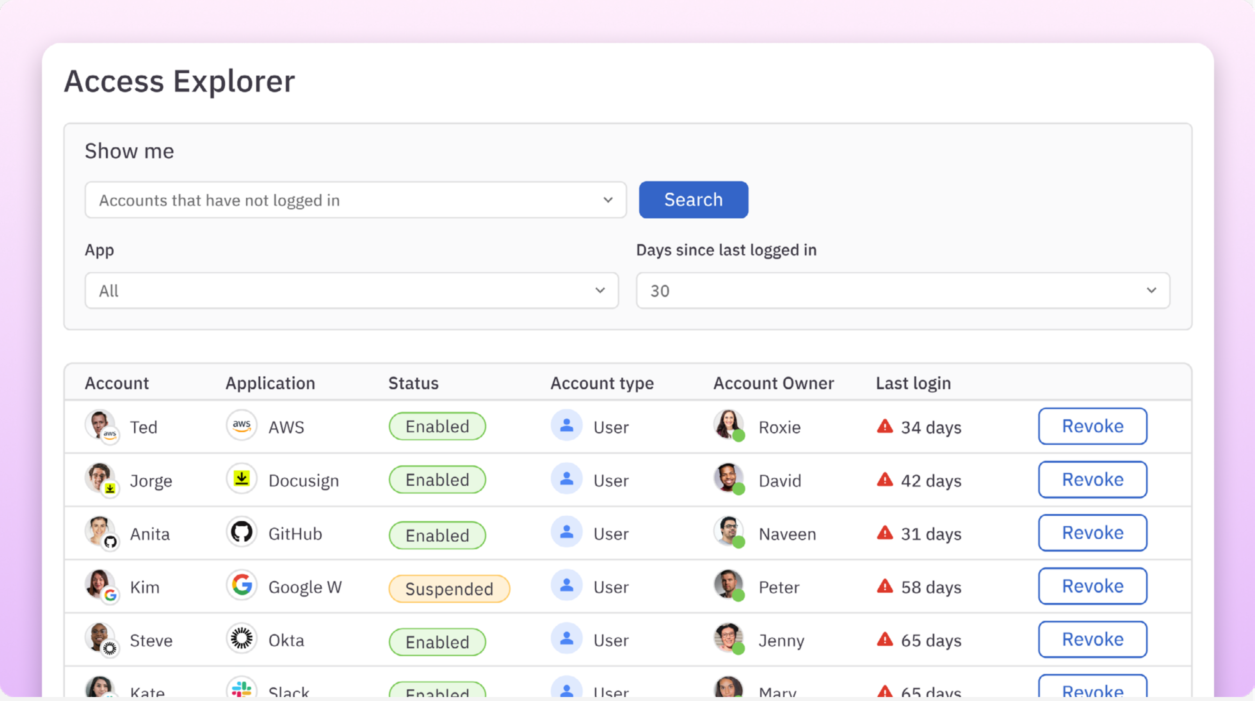


Shadow apps

These applications are in use by members of your organization

Application	Status	Accounts	First discovered	Last accessed
Trello	Discovered	6	Jan 9, 2024	Jan 9, 2024
Docusign	Ignored	6	Jan 4, 2024	Jan 8, 2024
GitHub	Discovered	6	Jan 2, 2024	Jan 2, 2024
ChatGPT	Discovered	6	Dec 23, 2023	Jan 9, 2024
Figma	Ignored	6	Dec 14, 2023	Dec 20, 2023
Jira	Ignored	6	Dec 10, 2023	Jan 12, 2023

💡**Did you know?** ConductorOne helps you eliminate unnecessary SaaS spend. Lower your overall SaaS costs by bringing shadow apps under management. Eliminate unnecessary apps, control access, and monitor ongoing usage.



Access Explorer

Show me

Accounts that have not logged in

App: All

Days since last logged in: 30

Account	Application	Status	Account type	Account Owner	Last login	
Ted	AWS	Enabled	User	Roxie	⚠ 34 days	Revoke
Jorge	Docusign	Enabled	User	David	⚠ 42 days	Revoke
Anita	GitHub	Enabled	User	Naveen	⚠ 31 days	Revoke
Kim	Google W	Suspended	User	Peter	⚠ 58 days	Revoke
Steve	Okta	Enabled	User	Jenny	⚠ 65 days	Revoke
Kate	Slack	Enabled	User	Mary	⚠ 65 days	Revoke

Learn more about ConductorOne

Watch → How Ramp enforces least privilege | ConductorOne Customer Spotlight

2. SailPoint IdentityIQ

SailPoint IdentityIQ is an advanced identity governance solution tailored for complex enterprise environments to automate and secure user access and identity management across various systems. It does this by leveraging AI and machine learning for predictive identity functionalities, allowing organizations to detect and respond to strange access patterns.

The solution offers a robust set of capabilities, including user access discovery, role-based access control (RBAC), segregation of duties (SoD) enforcement, access request and approval workflows, and more. These features automate the processes involved when employees join, move within, or leave an organization — ensuring continuous compliance and security.

In addition, IdentityIQ integrates with various IT environments through SailPoint's extensive connector library, supporting both on-premises and cloud applications.

Features of SailPoint IdentityIQ

SailPoint IdentityIQ offers two distinct features:

→ **Lifecycle Management.** This feature simplifies user access requests through a self-service portal, allowing users to request access as needed. This process is supported by automated provisioning (creation and setup) and deprovisioning (revocation and removal) of access rights and accounts across all connected systems.

→ **Compliance Management.** This simplifies compliance processes by automating access certifications and allowing managers and auditors to periodically review and verify user access rights. It also provides tools for managers to approve, revoke, or modify user access. They can choose to schedule this process regularly (e.g., quarterly, annually) and can also customize it to suit the specific data compliance requirements of the organization.

Other features include:

→ SailPoint extension modules and add-ons:

- **SailPoint Password Manager**. Enables users to manage and reset their passwords.
- **SailPoint File Access Manager for Data Access Governance**. Provides secure access to regulated and unstructured data.
- **SailPoint Access Risk Management**. Unifies access control across multiple applications such as SAP ERP, SAP SuccessFactors, S/4HANA and more.
- **SailPoint SaaS Management**. Visibility into hidden and over-provisioned accounts in SaaS environments.

3. Microsoft Entra

Microsoft Entra is a comprehensive identity and access management suite designed to secure, manage, and govern access across various environments, from cloud-based systems to hybrid settings.

Entra integrates several components, including the rebranded Azure Active Directory (now Microsoft Entra ID), which handles billions of authentications daily. This integration helps manage user and workload identities, apps, and devices, securing them through multi-factor authentication (MFA), single sign-on (SSO), and conditional access policies.

One of Microsoft Entra's standout features is its support for decentralized identity through Microsoft Entra Verified ID. This platform uses blockchain technology to enable user-owned digital identities that can be verified without central authority, providing greater privacy and control over personal data. It also supports verifiable credentials that users can manage and present through Microsoft Authenticator, integrating seamlessly with applications across various platforms.
Workload ID helps secure applications and their connections to cloud resources, ensuring that only authorized services can access sensitive data.

Features of Microsoft Entra

→ **Permissions Management**. As part of its cloud infrastructure entitlement management (CIEM) capabilities, Entra offers detailed visibility and control over permissions across Microsoft Azure, Amazon Web Services (AWS), and Google Cloud Platform (GCP).

→ **Workload ID**. Entra provides identities for applications and services, allowing secure access to cloud resources and facilitating secure interactions between different tech stacks.

→ **Domain Services**. This gives you access to managed domain services—such as Windows Domain Join, group policy, LDAP, and Kerberos authentication—without having to deploy, manage, or patch domain controllers. You also enjoy a 'lift-and-shift' migration of legacy applications from your on-premises environment to a managed domain.

→ **Identity Governance**. Provides tools for managing the entire lifecycle of employee identities, from creation based on HR system signals to removal when an employee leaves the organization. It also enables secure access for guest and partner identities.

4. CyberArk Identity

CyberArk Identity is an identity and access management (IAM) solution that provides comprehensive security features to manage and secure identities across an enterprise. This solution integrates various functionalities to safeguard human and machine identities, ensuring secure access to resources irrespective of location.

The platform offers privileged access management (PAM), allowing organizations to control, monitor, and secure access to critical systems and data. Key features include the management of privileged credentials, session security, and threat detection, which are vital to preventing unauthorized access and mitigating insider threats.

CyberArk Identity also offers advanced features like just-in-time access, reducing the risk associated with permanent privileged access by granting privileges on an as-needed basis.

Additionally, for endpoint security, CyberArk provides tools that help organizations enforce least privilege policies and secure credentials on endpoints, which are critical for protecting against ransomware and other malware attacks

Features of CyberArk Identity

→ **Identity Connector**. Helps integrate with on-premise directories and internal web applications, allowing RADIUS authentication without a VPN. Plus, it enhances security by issuing unique PKI Certificates to each tenant, encrypting communications, and ensuring all data transfers with the CyberArk Cloud are over TLS 1.2, making them unreadable by AWS infrastructure.

→ **User and Admin Portal** Security. CyberArk Identity allows user authentication through its directory, external directories like Active Directory, or external Identity Providers. It implements password rules via built-in or external policies or SAML integration. The Admin Portal is protected with security features such as CAPTCHA, security images, adaptive MFA, and defenses against login attacks. Additionally, CyberArk supports third-party MFA solutions and controls administrative access through specific roles and permissions.

→ **CyberArk Cloud Agent Security**. connect to the Internet using corporate settings and securely communicate with the CyberArk Identity tenant. All communications, including data transmission and “keep alive” checks, are encrypted using SSL/TLS. The HTTPS connection utilizes TLS 1.2 or higher Cipher Suites, ensuring that all data exchanged with the CyberArk cloud is encrypted in transit.

5. Ping Identity

Ping Identity is an all-in-one identity and access management (IAM) platform for complex enterprise environments. It has multiple authentication methods, including the PingID mobile application for Apple and Android devices, which is fully managed by Ping Identity, the PingID desktop app and PingID APIs.

Ping Identity can also handle different identity scenarios across large-scale deployments, supporting thousands of SaaS and on-premises applications, which helps streamline authentication processes and reduce administrative overhead.

Features of Ping Identity

- **PingOne Credentials**. Enables organizations to create, issue, manage, and revoke digital verifiable credentials (VCs) from a unified interface. These credentials, which include identification records, entitlements, and authorizations, allow service providers to instantly verify their authenticity and integrity at the time of use. The system also allows for customizing and automatic issuance of credentials based on predefined attributes, ensuring that each credential contains essential information such as the issuer, recipient, and specific data attributes. In addition, these credentials are cryptographically secure, guaranteeing their provenance and safeguarding against tampering.
- **Ping Identity Verification**. This offers solutions such as; quick matching of a live-face capture with a government ID, easy integration of identity verification into applications and workflows, automating the form-filling process with verified attributes, and enabling seamless linking of digital identities to devices or credentials.
- **Selfie Matching**. users are prompted to submit a selfie, which is then passively checked for liveness using ISO-certified technology to ensure authenticity.
- **PingOne Protect**. This feature utilizes a comprehensive set of risk predictors to calculate an overall risk score, which then informs the enforcement of various security measures based on user behavior and potential threats. These measures can include CAPTCHA, password resets, selfie verification, and push notifications, tailored to the assessed risk. The system optimizes individual predictors, combines them, and integrates third-party signals, allowing for the creation of custom overrides. Key predictors include bot detection, IP and user velocity, geolocation anomalies, IP reputation, the use of anonymous networks, user risk behaviors, device-based anomalies, and both custom and composite third-party predictors.

6. ManageEngine ADAudit Plus

ManageEngine ADAudit Plus is an auditing and security compliance tool tailored for Windows Active Directory environments. This solution offers real-time monitoring capabilities, user and entity behavior analytics (UEBA), and detailed change audit reports.

ADAudit Plus excels in tracking all changes to Windows Active Directory objects such as users, groups, computers, GPOs, and organizational units. Its ability to provide a single, correlated view of activities across hybrid AD environments makes it a great tool for enterprises needing to oversee both on-premises and cloud-based resources.

Features of ManageEngine ADAudit Plus

→ **Active Directory Auditing**. ADAudit Plus offers real-time auditing of Active Directory environments, allowing you to monitor user activities and changes to AD objects like users, groups, computers, GPOs, and organizational units. It helps track both successful and failed login attempts, providing detailed insights into user behavior and potential security risks.

→ **Multi-platform Support**. In addition to Active Directory, ADAudit Plus extends its auditing capabilities to Azure AD, Windows servers, workstations, and file servers. It supports various file server platforms, including NetApp, EMC, Synology, Hitachi, and Huawei, among others. This provides a unified solution for auditing across a hybrid IT environment.

→ **Privileged User Monitoring**. This oversees and audits administrator actions across various aspects like AD schema, users, groups, OUs, and GPOs. It ensures compliance with IT regulations by keeping an audit trail of privileged user activities within the domain. The system detects privilege escalation by documenting first-time privilege use and assessing the necessity of a user's privileges. It also identifies behavioral anomalies by monitoring deviations from normal access patterns, which helps spot attackers using compromised privileged accounts.

→ **File Change Monitoring**. This involves real-time tracking of file and folder access activities, including actions like create, read, delete, modify, and move. It also audits permission changes by noting old and new NTFS and shares permission values, and monitors file integrity by alerting on suspicious changes to critical system files. Additionally, it reports on all accesses and changes to shared files, detailing who accessed what, when, and from where. This system helps streamline compliance audits with ready reports for standards like HIPAA, GDPR, and ISO 27001, and is compatible across various platforms such as Windows servers and NetApp filers.

7. Lumos

Lumos is a SaaS management and identity governance platform that streamlines IT operations and enhances security within organizations. It integrates various functionalities under a single platform, making it simpler to manage software access and vendors, as well as to automate IT tasks like help desk operations, access requests, and provisioning.

One of Lumos's distinct features is automating IT operations to reduce IT tickets and improve time-to-resolution for access issues. It also allows organizations to enforce least privilege access control, ensuring that employees have access only to the resources necessary for their roles. Additionally, Lumos supports multi-stage approvals for access requests, which can include security training completion as part of the access criteria.

As part of a way to further aid in compliance and audit readiness, Lumos by simplifies access reviews by providing one-click audit reports to satisfy auditor requirements. Its platform can detect redundant apps and unused accounts, enabling organizations to reduce SaaS spending by removing or renegotiating these resources.

Features of Lumos

→ **Identity Governance**. The platform automates user access reviews and integrates them with compliance reporting for standards like SOX, SOC 2, and ISO 27001. This simplifies managing user permissions, ensuring that access is granted appropriately and revoked when no longer needed.

→ **Automated Access Revocation**. Lumos enables the deprovisioning of access for users whose permissions are rejected. This is achieved through direct integrations with your Identity Provider (IdP) or associated applications. Alternatively, the system can notify application administrators to revoke access manually. To ensure compliance and maintain records, administrators must upload documentation verifying the completion of the revocation process, thereby enhancing security protocols and accountability.

→ **Centralized Access Data Repository**. Lumos consolidates critical employee information, such as role assumption dates, into a unified source of truth. It integrates seamlessly with your identity provider to import Single Sign-On (SSO) group data and retrieves comprehensive entitlement data directly from both enterprise and cloud-based applications, including NetSuite CRUD permissions and AWS IAM groups. Additionally, the system supports integrating employee data from various other applications through customizable API connectors for enhanced flexibility.

→ **Streamlined Delegated Reviews**. Enhances access management by enabling the delegation of reviews to relevant stakeholders such as managers, application, or role owners. To ensure the timely completion of access reviews, the system automates the dispatch of notifications and reminders via email or Slack.

8. LogicManager

LogicManager is a comprehensive governance, risk, and compliance (GRC) platform designed to streamline processes and enhance the efficiency of risk management within organizations. It offers a robust set of features, including Enterprise Risk Management (ERM), incident management, and extensive risk and readiness libraries which support a wide range of compliance frameworks.

LogicManager's user access review functionalities work on the principle of least privilege to counter security vulnerabilities. They also include vendor spend management to validate proper delegation of license levels and identify redundant license expenses.

Features of Logic Manager

→ **Enhanced Risk Management Framework**. LogicManager's Custom Profile & Visibility Rules feature enables organizations to accurately assess the risk levels and characteristics of both applications and physical resources. Additionally, the system facilitates the implementation of controls to mitigate identified risks and establishes criteria for determining the frequency of access reviews.

→ **Advanced Integration Hub**: This hub streamlines the management of entitlement change tickets by enabling automation within the LogicManager Workflow system. It supports direct integrations with tools such as Jira and Active Directory solutions like Azure.

→ **Automated Event Management System**. The Event Management system within LogicManager streamlines the engagement of managers in reviewing employee entitlements through integration with your established file transfer processes. By simply uploading a file to an SFTP server, the system automatically generates a LogicManager event — which then initiates a review and sign-off process.

9. SecurEnds

SecurEnds is a cloud-based identity governance and administration platform that specializes in automating user access reviews, entitlement audits, and access certifications. The platform is designed to support compliance with several audit requirements.

The key features of SecurEnds include the automation of Credential and Entitlement Management (CEM), which enables organizations to enforce and revoke access rights efficiently. This automation extends to integrating with different systems such as Active Directory, Office 365, and major cloud services, facilitating a centralized management approach.

Features of SecurEnds

- **Unified Identity Repository with Advanced Matching**. This feature employs fuzzy logic to accurately unify and match identities from various systems of record within a single repository. By integrating credentials and entitlements from across the organization, it provides a comprehensive view of user identities.
- **Identity-Centric Mind Map**. This tool provides a visual representation that illustrates "*who has access to what*" within an organization, enhancing visibility into access controls. It features dynamic filtering capabilities, allowing users to navigate and refine views by specific user, |application, or entitlement.
- **Flexible Review Management System**. This system supports various review types and accommodates roles such as direct managers, entitlement custodians, application managers, and ad-hoc reviewers.
- **Audit Trail with Integrated Remediation**. This feature provides a centralized audit trail by logging all approval and revocation decisions, along with reviewer notes, within an ITSM-based framework. The built-in remediation functionality facilitates immediate corrective actions and compliance management.

UAR Software Functionality

User Access Discovery and Inventory

This is simply the process of identifying and documenting all user access permissions within an organization's IT environment.

This functionality is designed to create a comprehensive and up-to-date inventory of all users and their corresponding access rights across all systems, applications, and data.

Key components of this functionality include:

Data Collection

→ The software identifies various sources of user access data, such as directories (e.g., Active Directory, LDAP), databases, cloud services, and application-specific user accounts.

→ Automated tools extract user data, including user names, roles, group memberships, and specific permissions from each identified source.

→ The software has the ability to integrate with multiple platforms (e.g., Windows, Unix/Linux, cloud platforms like AWS, and Azure) to ensure comprehensive data collection.

Data Aggregation

→ Collected data is consolidated into a central repository to facilitate easy access and management.

→ Data from different sources is normalized into a standard format, enabling uniform analysis and reporting.

User and Access Identification

→ The software resolves identities by linking multiple user accounts belonging to the same individual across different systems.

→ Analyzes user roles and permissions to determine access levels. This includes mapping users to roles and the permissions those roles entail.

Permissions Mapping

→ Detailed cataloging of what specific permissions entail, across various systems, to provide clear visibility into access scopes.

→ Establishes clear definitions for each role within the organization and aligns them with corresponding permissions and access rights.

Role-Based Access Control (RBAC) Enforcement

RBAC enforcement is the process through which resource access is controlled under a model where rights are granted to roles rather than to individual users.

These roles represent a set of permissions that align with the responsibilities and needs of the users in those roles. Implementing RBAC effectively reduces the risk of unauthorized access and streamlines the management of user permissions.

To enforce RBAC:

- → Define roles based on job functions within the organization. Each role should have permissions that allow a user to perform specific job duties.
- → Assign attributes to roles such as role name, description, associated permissions, and conditions under which the permissions apply.
- → Establish a hierarchy of roles to manage role inheritance, where higher-level roles automatically include the permissions of their junior roles.
- → Specify capabilities assigned to each role, such as read, write, or delete access to particular systems or data.

💡 **Pro Tip →** Implement the Principle of Least Privilege (PoLP) to ensure permissions are strictly aligned with the minimum necessary for users to fulfill their job functions, avoiding excess rights that could lead to security vulnerabilities.

Segregation of Duties (SoD) Compliance

This involves implementing policies and procedures that prevent conflicts of interest by separating critical functions among different employees or departments. This functionality is essential for ensuring financial integrity, regulatory compliance, and internal security within an organization.

Key components include:

Identification of Conflicting Duties

- → Identifying and documenting potential risks associated with individual roles or processes. This can include mapping out roles and responsibilities to identify where conflicts of interest or fraud risks may exist, such as the same person having access to both creating and approving financial transactions.

Role Design and Adjustment

- → Design organizational roles to divide duties among different employees or departments appropriately.
- → For example, separating the roles involved in ordering, receiving, and paying for goods and services.
- → Adjusting roles to fit organizational needs while maintaining compliance with SoD principles, ensuring that no role has conflicting permissions.

Control Mechanisms

→ Implementing controls that prevent conflicts of interest, such as automated checks within software systems that block unauthorized actions based on role settings.

→ Systems are in place to detect and alert potential SoD violations after they occur, often through continuous monitoring and regular audits.

Access Request and Approval Workflows

Access request and approval workflows are processes designed to control how access to various systems and data is requested, reviewed, and granted or denied.

These workflows help maintain security and compliance by ensuring that access is only provided based on legitimate business needs and in accordance with established security policies.

Key components include:

Request Submission

→ A user-friendly interface for submitting access requests, which includes forms to fill out detailing the specific access needed and the reason for the request.

→ Dynamically generated request forms that adjust based on the requester's role and the context of the access requirement.

Review Process

→ Establishment of a multi-tier review process that routes requests to the appropriate managers or role owners for approval. This may include direct supervisors, IT security teams, and compliance officers.

→ Conditional routing rules are based on the type of access requested, the data sensitivity, or other criteria that determine who must review and approve the request.

Approval Mechanisms

→ For low-risk requests, automated approval processes based on predefined policies can streamline access provisioning.

→ For high-risk or unusual requests, manual review by one or more approvers is required, ensuring that all aspects of the request are scrutinized.

User Provisioning and Deprovisioning

This is the process of granting, updating, and revoking user access to systems, applications, and data. This automated management of user access rights across an organization's IT environment is essential for operational efficiency, security, and compliance.

Provisioning Process

- → Automated creation of user accounts across various systems and applications when a new employee joins or changes roles within the organization.
- → Integration with RBAC to ensure users receive access based on predefined roles matching their job functions.
- → Utilization of access bundles or profiles that package together all necessary access rights for a specific role or department.

Deprovisioning Process

- → Automatic deactivation or deletion of user accounts when an employee leaves the organization or transitions away from roles requiring specific access.
- → Ensuring all access rights are removed or transferred following role changes or termination of employment to prevent unauthorized access.

Integration with Other Systems

- → Direct integration with human resources management systems to trigger provisioning or deprovisioning based on HR events like hiring, promotion, or termination.
- → Ensuring that provisioning and deprovisioning activities are logged and auditable to comply with internal and external regulations.

Entitlement Reviews and Certification

This is the process of reviewing and verifying user access rights within an organization. This process ensures that all users have appropriate access based on their current roles and responsibilities and that any discrepancies or unauthorized access are identified and rectified.

Key components include:

Entitlement Data Collection

- → Gathering detailed access data from across all systems, applications, and data repositories to form a complete picture of user entitlements.

Review Execution

- → Executing reviews based on roles or individual user access to ensure that rights are correctly aligned with job functions.
- → Utilizing automated tools to pre-analyze and flag potential issues, supplemented by manual reviews for complex or high-risk entitlements.

Certification and Decision Making

→ Implementing decision workflows where managers or compliance officers certify that the reviewed entitlements are correct or initiate changes where discrepancies are found.

→ Procedures for escalating unresolved issues or high-risk findings to higher management or specialized teams.

Remediation Actions

→ Automatically revoking or adjusting access rights based on review outcomes using predefined rules.

→ Processes for manual intervention when automated remediation is not suitable or requires additional oversight.

Security and Compliance

This part of the functionality provides tools and processes to support compliance with key regulations, secure data handling, and proactive security measures.

Here's an in-depth look at each component:

Support for Key Regulations

→ The software is designed to support compliance with major regulatory standards such as PCI DSS (Payment Card Industry Data Security Standard), GDPR (General Data Protection Regulation), HIPAA (Health Insurance Portability and Accountability Act), and SOX (Sarbanes-Oxley Act). It includes specific functionalities to address the unique requirements of each.

→ Features customizable control frameworks that can be adapted to the specific compliance needs of different regulations, including data handling, access controls, and audit processes.

Secure Authentication and Data Encryption

→ Implements strong authentication protocols, including multi-factor authentication (MFA) and single sign-on (SSO), to verify the identity of users accessing the system.

→ Utilizes robust encryption standards both at rest and in transit to protect sensitive information from unauthorized access and breaches.

→ Ensures the software is kept up-to-date with the latest security patches and updates to address new vulnerabilities as they arise.

Vulnerability Scanning and Threat Detection

→ Includes tools for continuously scanning the software environment to identify and assess vulnerabilities.

→ Employs advanced threat detection algorithms that monitor suspicious activities and potential threats in real-time.

→ Provides incident response capabilities allowing quick containment and remediation of detected threats, minimizing potential damage.

Audit Trails and Compliance Reporting

→ Automatically logs all user actions and system changes, providing detailed audit trails that can be critical during forensic analyses and compliance audits.

→ Generates comprehensive compliance reports that document adherence to regulatory standards, which can be critical during audits and reviews.

→ Features real-time compliance status monitoring with alerts that notify relevant personnel of potential compliance issues or lapses.

How to Choose the Right UAR Software (and What to Do Post-Purchase)

Define Your Requirements

Start by defining what you need from a UAR software.

→ **Scalability**. Ability to handle the growing number of users and complexities in your organization.

→ **Integration**. Compatibility with existing systems like HR databases, Active Directory, and other identity management frameworks.

→ **Automated Review Processes**. Features that automate the tedious parts of the access review process, like notifications, reminders, and report generation.

→ **Reporting and Analytics**. Advanced capabilities to generate insightful reports and analytics for audit trails and compliance purposes.

→ **User Interface**. Intuitive and easy-to-use interface for both administrators and end-users.

> 💡Create a checklist of must-have features versus nice-to-have features. This will help you prioritize your needs and make it easier to evaluate different software options against your specific requirements.

Evaluate Different UAR Software Options

Research and gather information on different UAR software options.
Look for:

→ **Vendor Reputation and Reliability**. Check reviews and testimonials to gauge the reliability and service quality of the vendor.

→ **Security Features**. Ensure the software has robust security measures in place, such as encryption, secure data storage, and regular security updates.

→ **Compliance Standards Supported**. Verify that the software supports compliance with relevant regulatory requirements.

→ **Pricing Model**. Understand the pricing structure—whether it is subscription-based, per-user, or a one-time fee.

💡 **Pro Tip →** Leverage industry forums, user groups, and professional networks to gather unbiased feedback and real-world experiences with different UAR tools. Hearing directly from current users can provide insights that aren't available through vendor materials alone.

Request a Demo

Before making a final decision, request demos and trial versions of the software from potential vendors. This allows you to:

→ See the software in action and check if it meets your requirements.

→ Evaluate the ease of use and functionality.

→ Determine how well it integrates with your existing systems.

💡 **Pro Tip →** During demos, simulate real scenarios that your organization might face. This approach helps assess how the software handles complex situations and reveals any potential shortcomings in a controlled environment.

Check for Customization and Support

Choose software that can be customized to fit the specific needs of your organization. Also, consider the level of customer support provided by the vendor, including:

→ **Availability of Support.** 24/7 support, response times, and available communication channels.

→ **Training and Documentation**. Availability of training sessions, user manuals, and online resources to help your team utilize the software effectively.

💡 **Pro Tip →** Ask potential vendors about the process for future updates and customizations. Ensure that the software can adapt to future technological advancements and changing regulatory requirements without excessive costs or disruptions.

Implement the Chosen Software

Once you've chosen a software, plan its implementation carefully. This involves:

→ **Setup and Configuration**. Installation of software, configuration of settings to match organizational policies, and integration with other systems.

→ **User Training**. Organizing training sessions for users involved in the UAR process to ensure they understand how to use the software effectively.

→ **Pilot Testing**. Running a pilot test with a small group of users to identify any issues and make necessary adjustments before full-scale deployment.

💡 **Pro Tip →** Develop a phased implementation plan that starts with a pilot program involving a diverse group of users. This method helps in identifying practical challenges and user resistance early, allowing for smoother organization-wide rollout.

Monitor and Evaluate

After implementation, continuously monitor the software's performance and effectiveness in simplifying the user access review process. Solicit feedback from users and use this information to refine your approach. Regular evaluation helps ensure that the software continues to meet your needs and compliance requirements.

💡 **Pro Tip →** Implement regular feedback loops with users to continually assess the effectiveness of the software. This can involve user surveys, focus groups, or feedback sessions. Use this data to advocate for necessary changes or upgrades with the vendor.

ConductorOne: The Ideal UAR Software

We've interacted with several clients over the past years — and we've highlighted a recurring theme: the lack of an effective user access review (UAR) system exposes organizations to serious security vulnerabilities and operational issues.

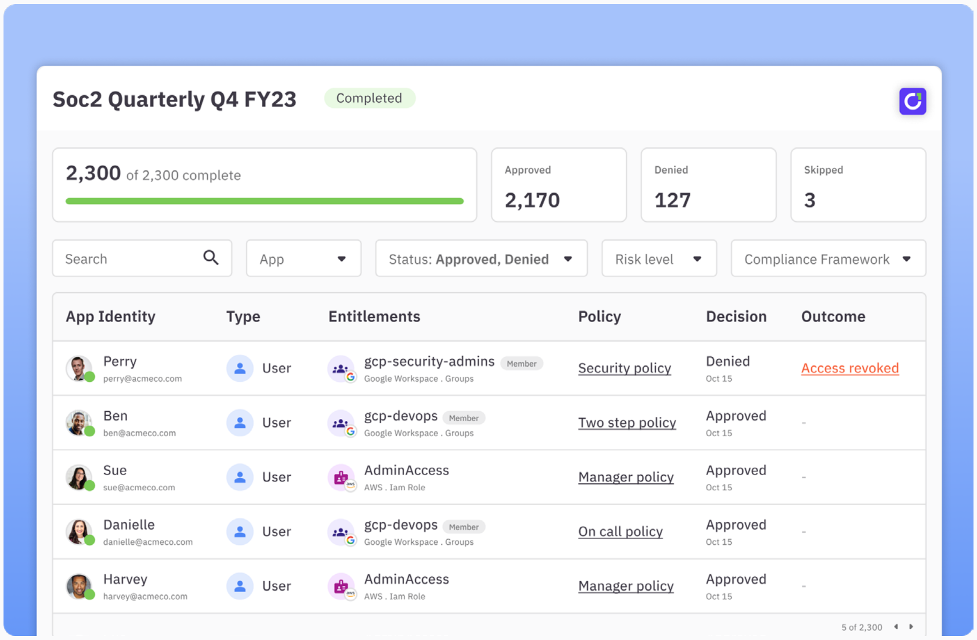
Many have shared troubling accounts, including wasteful allocation of resources, severe data breaches and leaks, compliance violations, and even long-lasting damage to their reputations.

Without a UAR process, it becomes nearly impossible to ensure that the right individuals have the right access at the right time.

ConductorOne addresses these challenges head-on by providing a streamlined, automated UAR platform designed with the needs of modern businesses in mind. Our solution reduces the administrative burden of conducting comprehensive user access reviews, thereby increasing the accuracy and timeliness of access permissions. By integrating advanced analytics and user-friendly workflows, ConductorOne ensures that user access rights are managed efficiently and in compliance with relevant regulations.

Why Do Customers Choose ConductorOne?

→ **Modern Experience**. Connect all of your applications with off-the-shelf integrations, run fully automated reviews, and notify reviewers in email or Slack.



Soc2 Quarterly Q4 FY23 Completed

2,300 of 2,300 complete

Approved 2,170

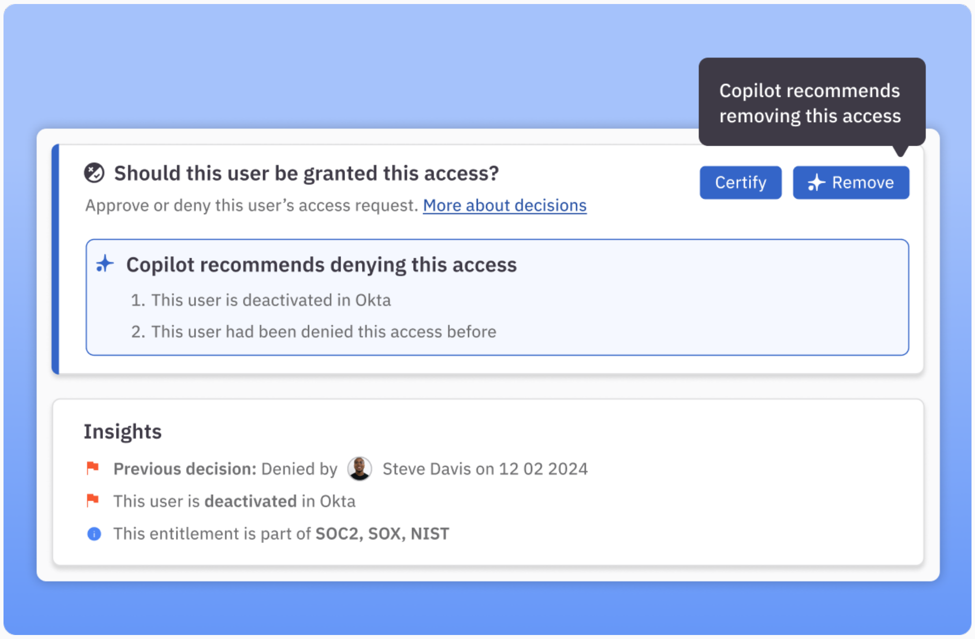
Denied 127

Skipped 3

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

5 of 2,300

→ **Risk Insights & Context.** Surface insights such as usage, risk level, and flags related to job title, department, and anomalous access for better review decisions.



Copilot recommends removing this access

Should this user be granted this access?

Approve or deny this user's access request. More about decisions

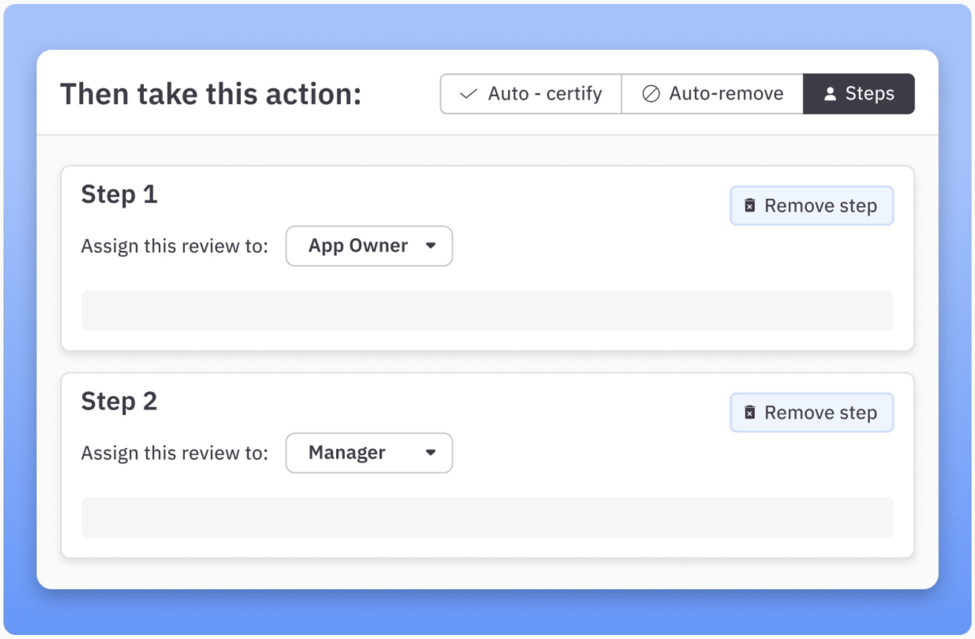
Copilot recommends denying this access

1. This user is deactivated in Okta
2. This user had been denied this access before

Insights

- **Previous decision:** Denied by Steve Davis on 12 02 2024
- This user is **deactivated** in Okta
- This entitlement is part of **SOC2, SOX, NIST**

→ **Configurable Review Workflows**. Build review workflows that meet your security needs with multiple reviewers and assign delegated reviewers in the event someone is out.



Then take this action:

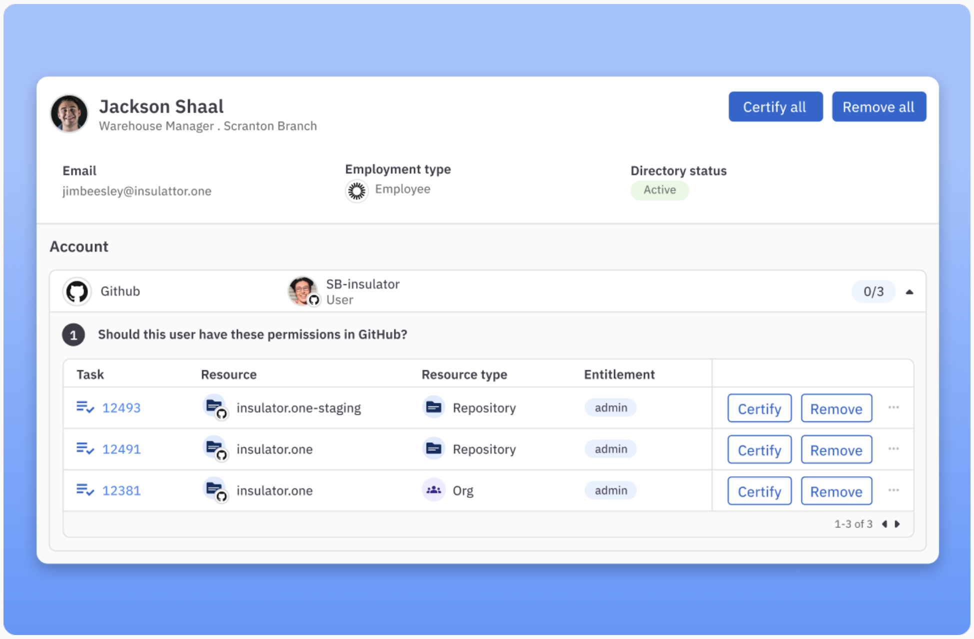
Step 1

Assign this review to: App Owner

Step 2

Assign this review to: Manager

→ **Streamlined Certifications**. Automatically approve low-risk access and utilize bulk approvals for a more streamlined review process.



Jackson Shaal
Warehouse Manager . Scranton Branch

Email
jimbeesley@insulattor.one

Employment type
Employee

Directory status
Active

Account

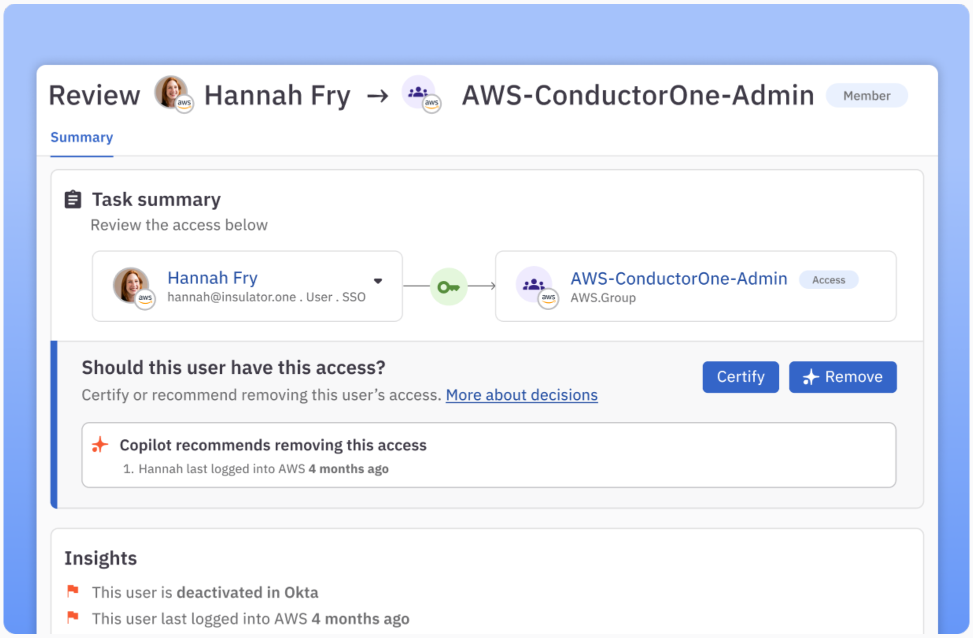
Github SB-insulator User 0/3

1 Should this user have these permissions in GitHub?

Task	Resource	Resource type	Entitlement	
12493	insulator.one-staging	Repository	admin	Certify Remove
12491	insulator.one	Repository	admin	Certify Remove
12381	insulator.one	Org	admin	Certify Remove

1-3 of 3

→ **Easy Revocations**. Automatically deprovision access through ConductorOne or kick off a manual revocation workflow.



Review Hannah Fry → AWS-ConductorOne-Admin Member

Summary

Task summary
Review the access below

Hannah Fry
hannah@insulator.one . User . SSO

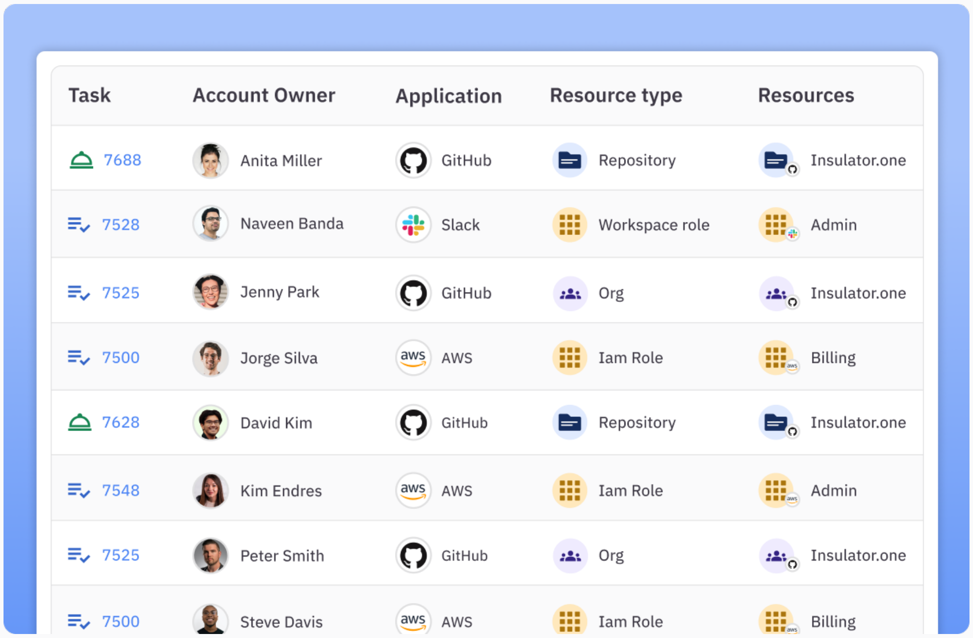
AWS-ConductorOne-Admin Access
AWS.Group

Should this user have this access?
Certify or recommend removing this user's access. More about decisions

Copilot recommends removing this access
1. Hannah last logged into AWS **4 months ago**

Insights
This user is **deactivated in Okta**
This user last logged into AWS **4 months ago**

→ **Full Audit Trail**. Population reports, access certification results, and remediation activity are fully tracked and ready for auditors with one-click reporting.



Task	Account Owner	Application	Resource type	Resources
7688	Anita Miller	GitHub	Repository	Insulator.one
7528	Naveen Banda	Slack	Workspace role	Admin
7525	Jenny Park	GitHub	Org	Insulator.one
7500	Jorge Silva	AWS	Iam Role	Billing
7628	David Kim	GitHub	Repository	Insulator.one
7548	Kim Endres	AWS	Iam Role	Admin
7525	Peter Smith	GitHub	Org	Insulator.one
7500	Steve Davis	AWS	Iam Role	Billing

Watch → How we use ConductorOne to run our own Access Reviews

We believe in ConductorOne — because we use it too.

Now, it's your turn to enjoy fully automated user access reviews

Try ConductorOne now

Get a demo