

CyberArk Secure Cloud Access

Manage cloud identities using Zero Standing Privileges.

Product overview

CyberArk Secure Cloud Access (SCA) gives cloud users secure, native access to AWS, Azure and GCP — without the risk of standing privileges or static credentials. With the SCA solution and the SCA MCP Server, organizations can take control of their cloud and AI adoption journey.

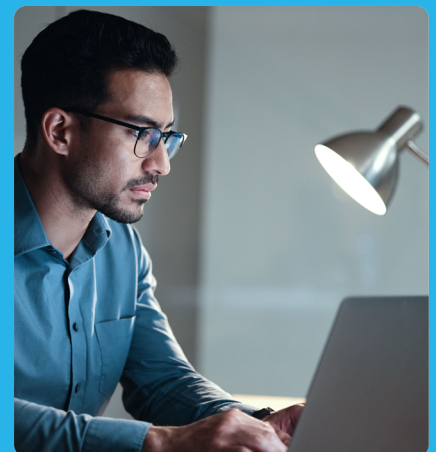
Built on Zero Standing Privileges (ZSP) and part of the CyberArk Identity Security Platform, the solution empowers developers, engineers, and cloud teams to work securely and quickly in their native tools — without disrupting productivity. At the same time, security teams can confidently adopt agentic workflows to maximize efficiency, eliminate credential sprawl across multi-cloud environments, satisfy audit requirements, and reduce the risk of credential compromise using dynamic access controls.

Core capabilities

- **Zero Standing Privileges:** Remove standing access with ZSP to reduce the risk of lateral movement and identity compromise using a combination of just-in-time access, elevated on-demand access, and granular control of Time, Entitlements, and Approvals (TEA).
- **Native User Experience:** Cloud users work as they prefer, with the help of AI developer tools like Amazon Q Developer, Claude Desktop, or any other client.
- **Integrate Across CSPs:** Unified controls and integrations across AWS, Azure, and GCP.
- **Workflow Automation:** Automate approvals and provisioning in ChatOps tools like Slack and ServiceNow.
- **Full Session Monitoring:** Record and monitor cloud sessions—console or CLI for streamlined auditing.

KEY BENEFITS

- **Reduced Risk:** ZSP capabilities enforced consistently across hybrid and multi-cloud environments reduces the risk of unauthorized cloud access and potential breaches.
- **Centralized Control:** One control plane with visibility across AWS, Azure, and GCP enforces ZSP everywhere — without requiring agents or introducing conflicting policies.
- **Simplified Audits:** Session monitoring and recording capabilities help fulfill compliance requirements like PCI DSS, NIST 800-53, and ISO 27001, reducing the potential for penalties.
- **Improved Operational Efficiency:** Drive innovation and optimize productivity with automated pipeline workflows and safe use of LLM and AI Agents during the development process.
- **Reduced Costs:** Automated controls minimize time and bandwidth strains on limited resources, optimizing the workforce efficiency and improving the bottom line.

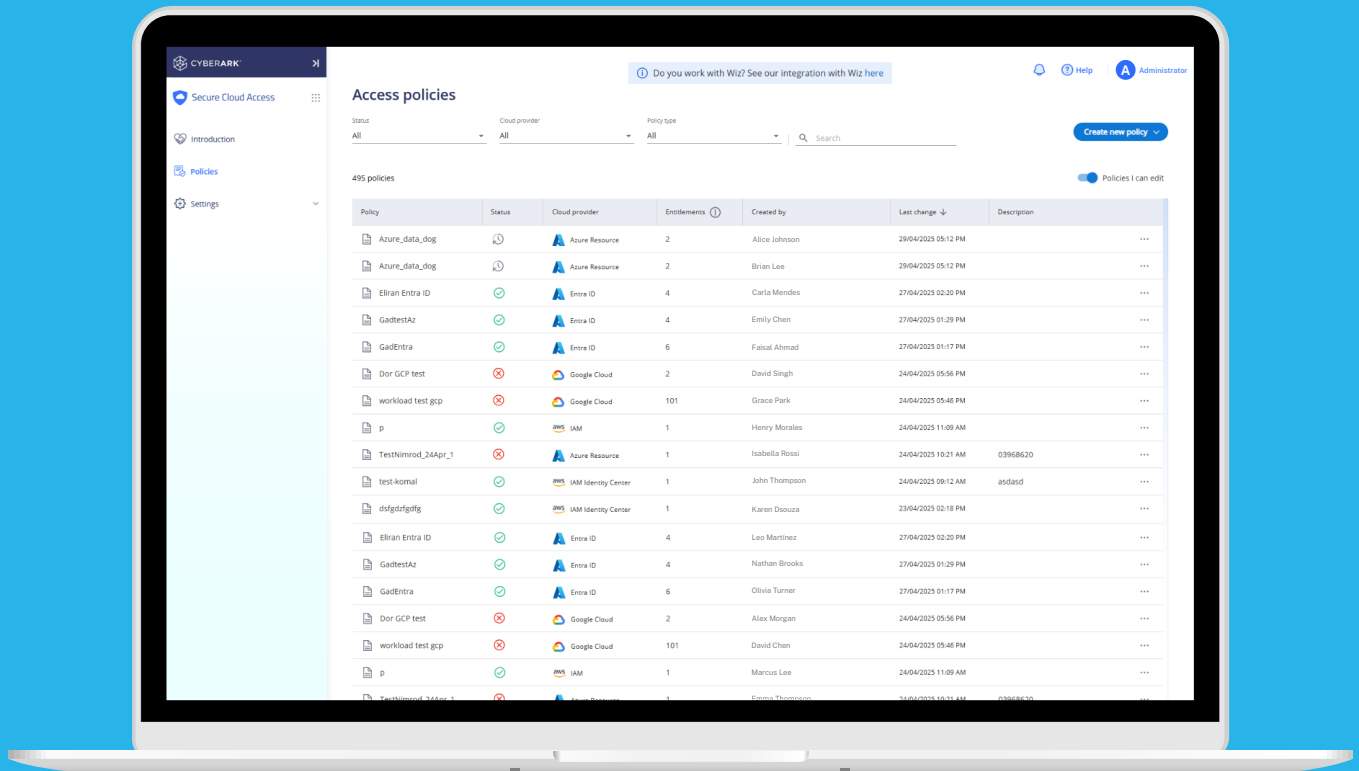


How it works

Secure Cloud Access applies ZSP, just-in-time entitlements, and scoped ephemeral credentials to a cloud user's federated identity — then revokes permissions automatically. No agents, no standing access, no risk of credential compromise.

Step by step: Secure Cloud Access

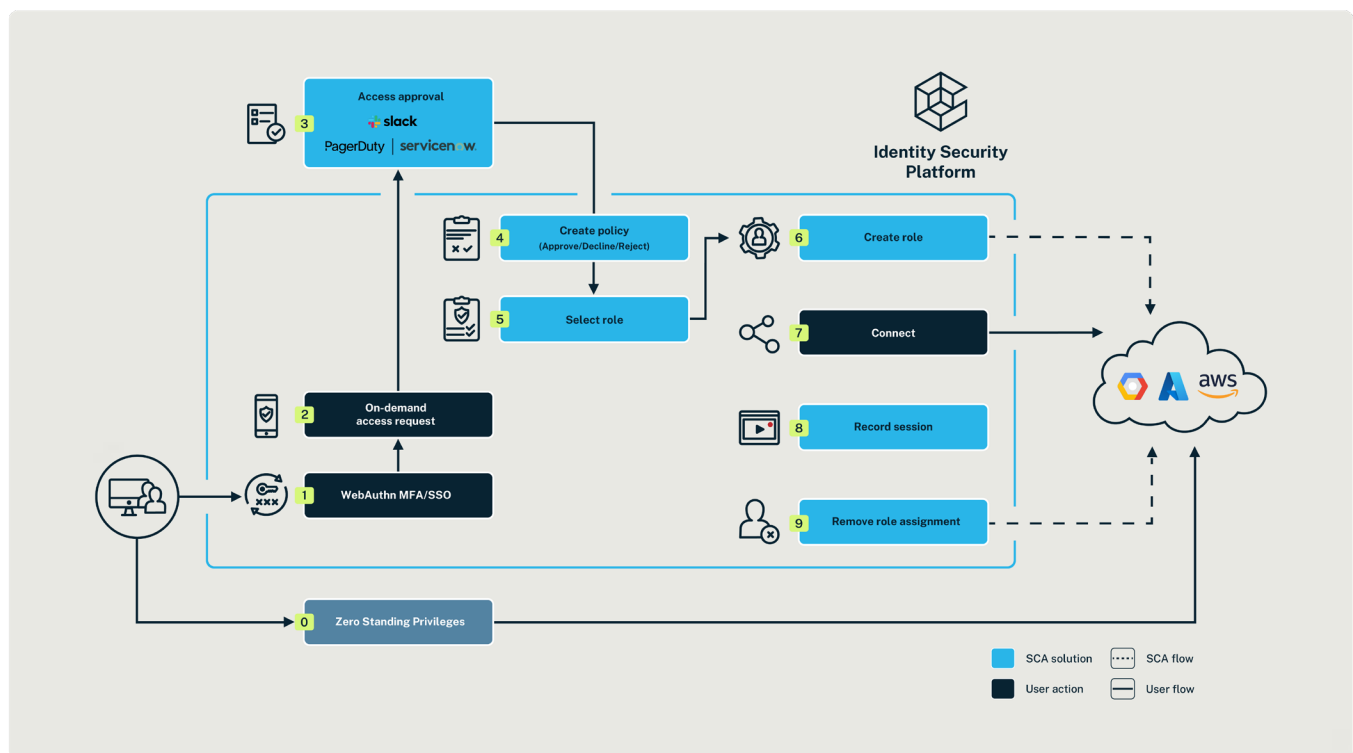
- 1. Login:** User authenticates via CyberArk or enterprise IdP.
- 2. Request:** After successful authentication, user requests access to the roles needed.
- 3. Elevate:** Access is approved and just-in-time entitlements are created.
- 4. Connect:** User connects via native CLI or cloud console and the session is recorded.
- 5. Revoke:** Entitlements provisioned are revoked automatically at the end of the access window.



Use cases: Examples of SCA in action

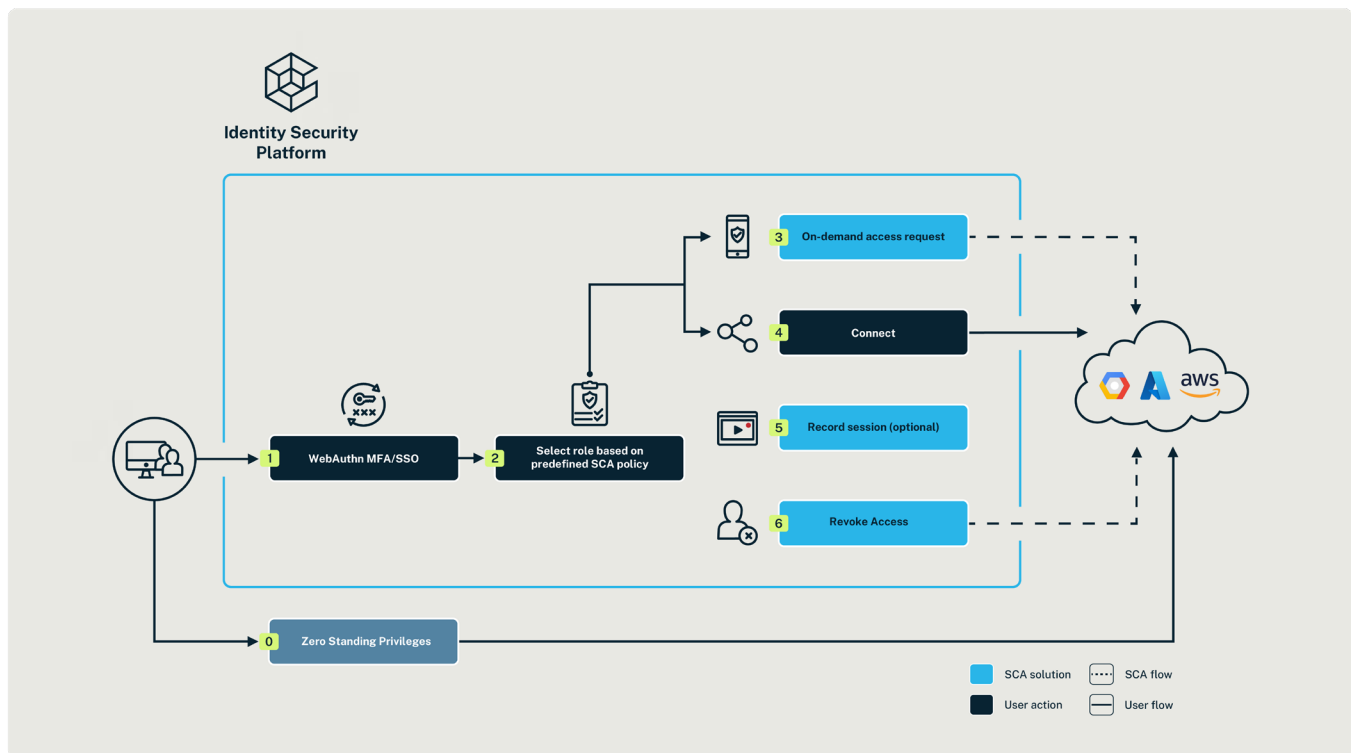
On-demand access

- **Incident-level access to production environments:** During an outage, SCA provides emergency ZSP access to the appropriate team members while maintaining full audit trails.
- **Elevated permissions for unplanned changes:** A cloud administrator needs to make configuration changes to a CSP they do not typically manage. They request permissions through SCA, which provides ZSP access to complete the task.



Pre-defined access

- **Multi-cloud resource management:** A CloudOps leader managing resources across AWS, Azure and GCP uses SCA to enforce consistent policies and centralize the administrator, user, and audit experiences.
- **Non-admin user access to sensitive data:** Third-party clinical researchers need access to patient data stored in Azure for a study. SCA provides time-bound ZSP access to ensure this data is only accessed for research purposes.



Secure Cloud Access provides secure, native access to the cloud using Zero Standing Privileges to remove persistent standing access and reduce risk — without disrupting user experience or developer velocity.

Explore our Secure Cloud Access demo <https://www.cyberark.com/try-buy/secure-cloud-access-demo/>

About CyberArk

CyberArk is the global leader in identity security. CyberArk's AI-powered Identity Security Platform helps organizations around the world reduce operational and security risks by enabling zero trust and least privilege with complete visibility, empowering all users and identities to securely access any resource, located anywhere, from everywhere. Learn more: [cyberark.com](https://www.cyberark.com).



©2025 CyberArk Software. All rights reserved. No portion of this publication may be reproduced in any form or by any means without the express written consent of CyberArk Software. CyberArk®, the CyberArk logo and other trade or service names appearing above are registered trademarks (or trademarks) of CyberArk Software in the U.S. and other jurisdictions. Any other trade and service names are the property of their respective owners. CyberArk believes the information in this document is accurate as of its publication date. The information is provided without any express, statutory, or implied warranties and is subject to change without notice. | U.S., 06.25 Doc. 1994494819