



클라우드 아이덴티티 보안 최고 전략

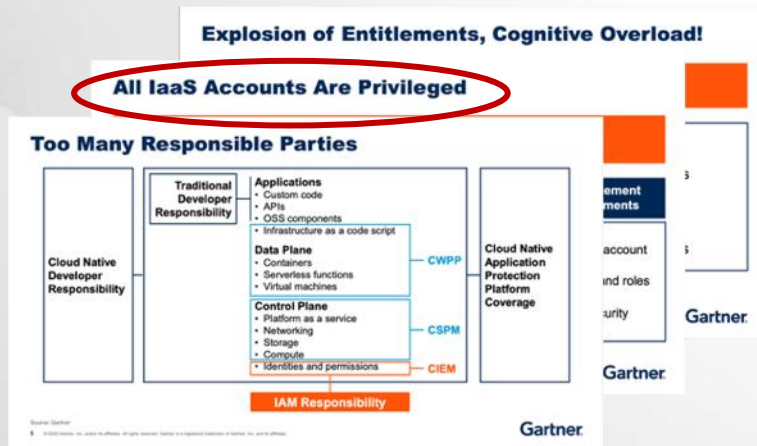
사이버아크 아이덴티티 솔루션



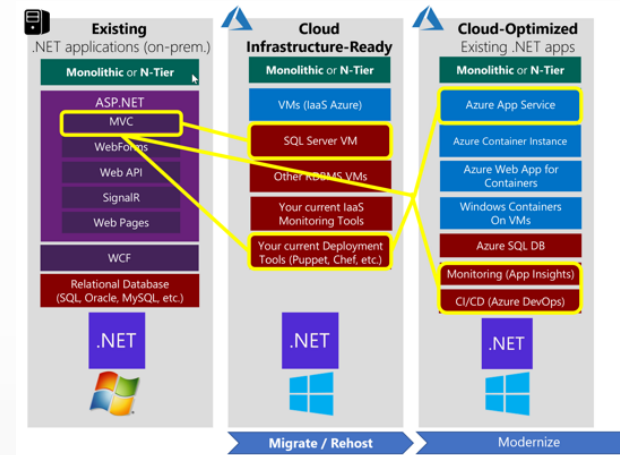
클라우드 환경의 현실과 보안의 필요성

클라우드 현실

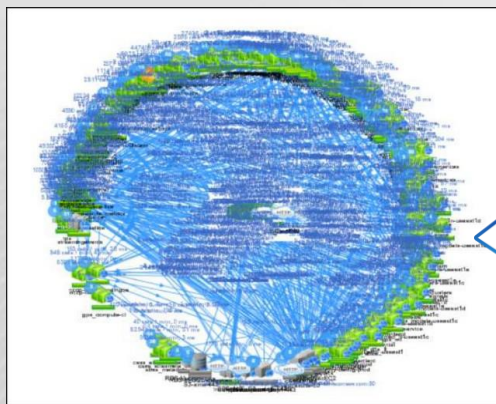
클라우드 환경에서의 역할 정의가 불명확



리프트 앤 쉬프트 개발 운영은 복잡



긴급한 상황에서의 확장된 권한 필요



"Um, something's broken."

모든 사람들(특히 엔지니어)은 속도를 요구



멀티 클라우드 채택

69%

2022

3 or more CSPs

60% Asia Pacific

92%

2023

3 or more CSPs

85% Asia Pacific

CyberArk Identity Security Maturity Model Report (Worldwide=1500)
(AP=423 | Australia=73 | Hong Kong=77 | India=48 | Japan=73 | Singapore=76 | Taiwan=76)
(EMEA=462 | Germany=104 | Israel=105 | Italy=49 | Netherlands=52 | Spain=47 | UK=105)
(Americas=615 | Canada=53 | Brazil=90 | Mexico=110 | US=362)



Hundreds of
Thousands of
IDENTITIES

Per average medium-to-large organizations

우리는 왜 클라우드 보안을 어려워하고 제로 트러스트 보안을 고려하나?

클라우드 보안

업무 환경 변화

많은 종류의 접속 장치

규수 준수

협업 필요

SaaS 업무 증가

오픈 네트워크

멀티 클라우드

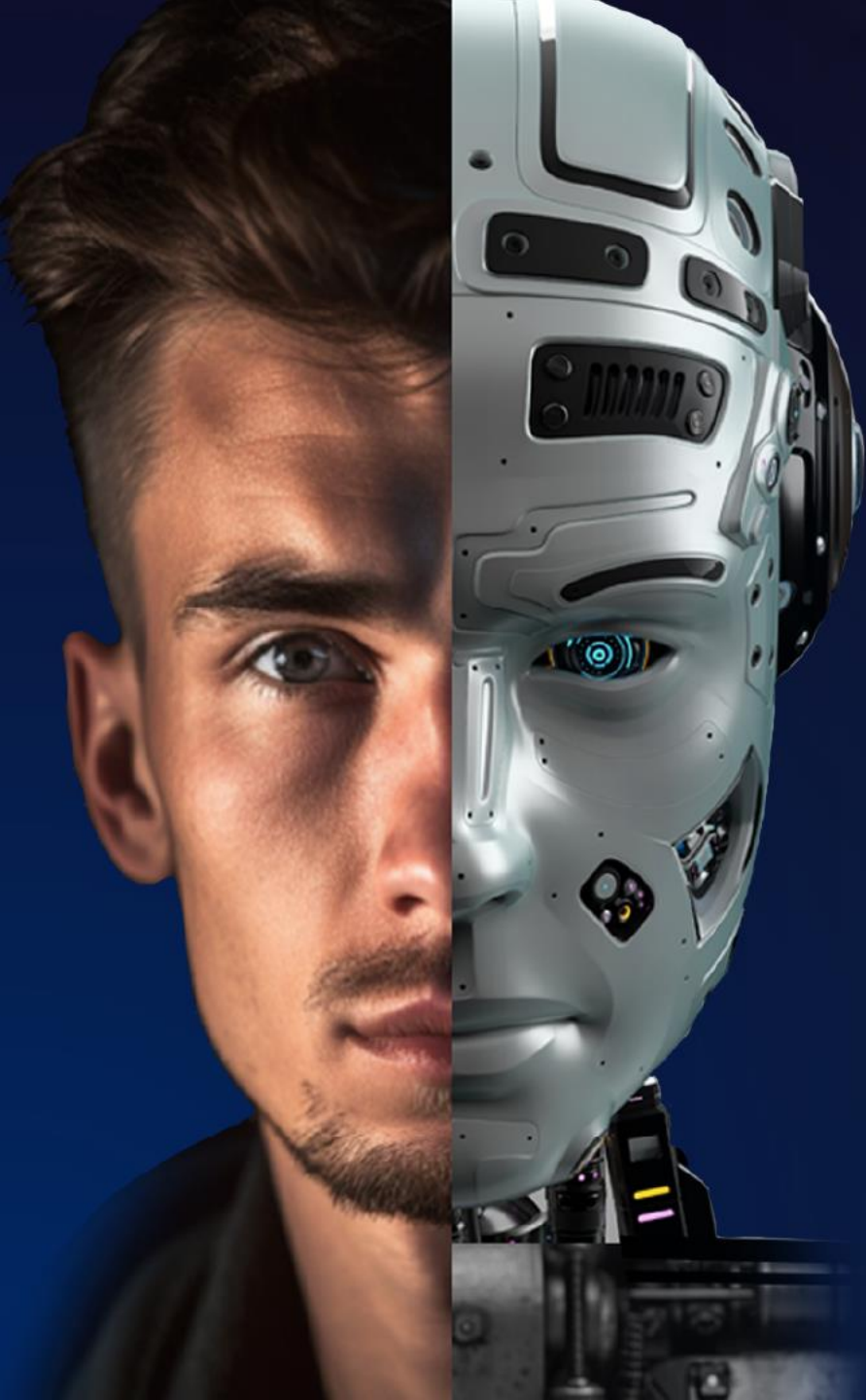
공격의 진화

시간/장소 제약이 없음

다양한 형태의 신원정보

제로 트러스트 기반





84% 이상 조직은 이미
아이덴티티 유출사고를
경험하고 있습니다.

클라우드 환경 보안을 위한 고려사항

클라우드 환경을 위한 보안

Identities



Admins



Workforce



Third Parties



Customers



DevOps



Workloads



Devices

Resources



Applications



Infrastructure



Consoles and services

Environments



클라우드 환경에서의 권한 관리 보안을 위한 주요 고려사항

- 과도한 권한부여로 인한 데이터 손실 및 유출 위험 감소
- 고정(영구적)권한을 줄이고 최소 권한 구현
- 사람 및 어플리케이션 접근에 대한 클라우드 접근 정책 관리
- 보안 및 규정 준수 유지
- 클라우드 Identity 활동 모니터링 및 감사

환경에 따른 차별화된 보안 방안

사용 사례

보안 방안

환경

SaaS 어플리케이션에 대한
고위험 접속 보안

세션 보호 및 모니터링



클라우드 VM상에서 운영되는
모든 워크로드 접속 보안

고정 사용 계정 및 시스템
접속을 위한 아이덴티티
관리 및 세션 연결 이원화



클라우드 인프라(IaaS)에
있는 워크로드 접속에
대한 보안

Dynamic, just-in-time access
(동적인 즉시 접속 제어)



클라우드 제공업자 콘솔
접속에 대한 보안 제어

네이티브 연결 및
최소권한 접속 관리





Identity Security Platform

Identities



Admins



Workforce



Third Parties



Customers



DevOps



Workloads



Devices

모든 신원정보에 대한
원활하고 안전한 접속

지능적인
특권 제어

유연한 신원
자동화 및 조정



Workforce &
Customer Access



Endpoint
Privilege Security



Privileged
Access Management



Secrets
Management



Cloud
Privilege Security



Identity
Management

Identity Security Intelligence



공통 서비스
플랫폼

단일 관리자
포탈

워크 플로우

통합 감사

인증 및 인가

SaaS

Hybrid

Self-Hosted

Resources



Applications &
Services



Infrastructure &
Endpoints



Data

Environments



Data Centers



OT



Hybrid & Multi-Cloud



SaaS

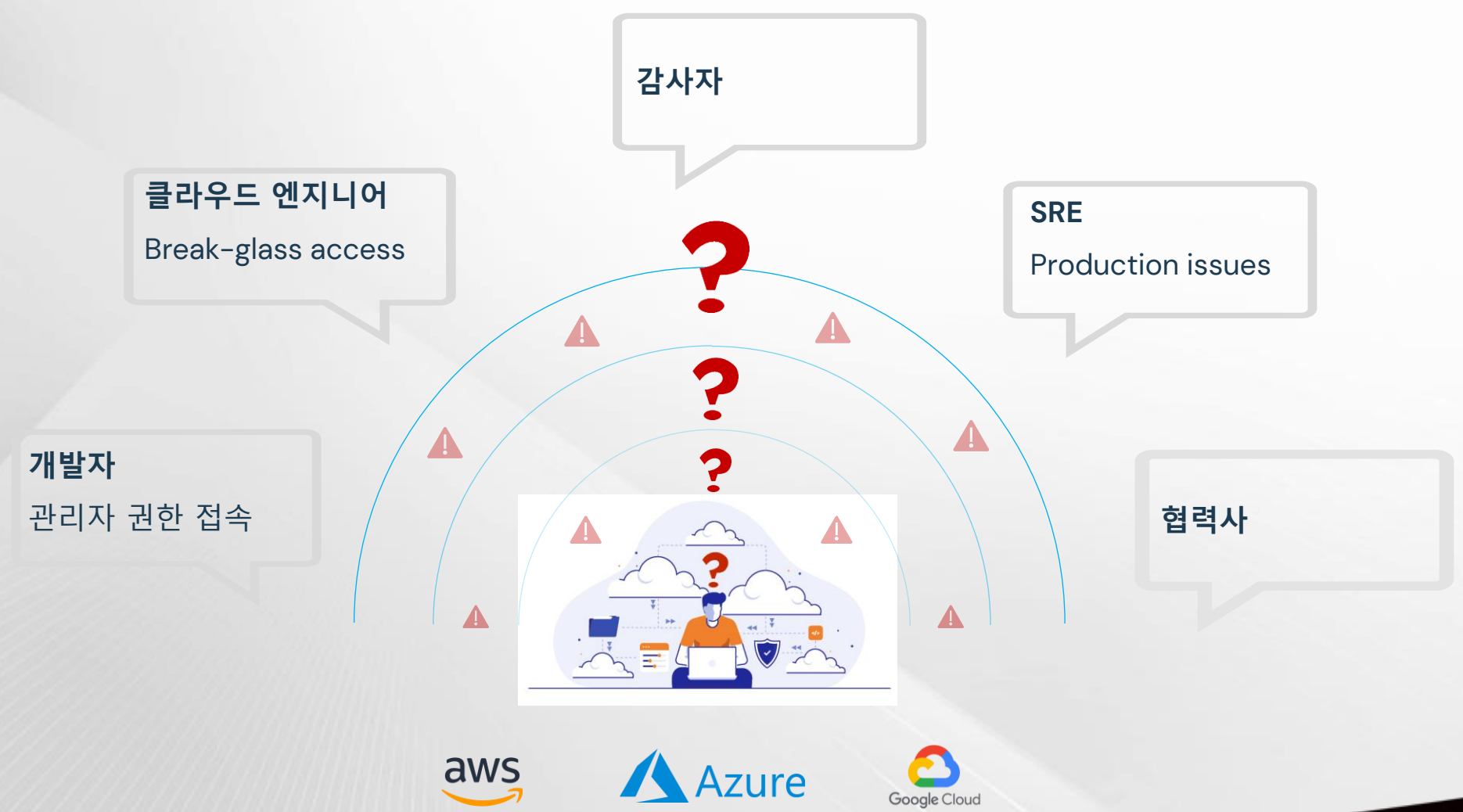
조직 관리자 및 사용자들을 위한 완벽한 통합 UI

The image displays two overlapping screenshots of the CyberArk user interface. The background screenshot shows the 'Dynamic Privileged Access' dashboard, featuring a navigation sidebar with options like 'Introduction', 'Recurring access', and 'Connectors'. The main content area displays a grid of service tiles including 'Privileged Cloud', 'Remote Access', 'Cloud Entitlements Manager', 'Endpoint Privileged Manager', 'Conjur Cloud', 'Application Administration', 'Secure Web Sessions', 'User Portal', 'General Setup', 'Identity Administration', 'Activities and Recordings', and 'Identity Security Analytics'. A 'Welcome to CyberArk' message and user information are visible at the top.

The foreground screenshot shows the 'Identity User Portal' interface. It features a sidebar with navigation options such as 'All Items', 'Devices', 'Activity', 'Account', and 'Identity Certification'. The main area is titled 'All Items' and displays a grid of application tiles for various services, including Amazon Web Services, AWS SCA SE APJ 7035, Need Help?, CYBERARK Identity Training, CYBERARK Documentation, O365 Portal, SmartFile, CYBERARK Developer Portal, Quick Demo Guide, Endpoint Privilege..., Rapid 7, GCP SE Global, CYBERARK Cloud Status, AWS SE APJ 7035, Tenable, ServiceNow, Postman, CYBERARK Release Notes, PWA Remote Access, Amazon WorkDocs, Vendor PAM Mobile, and others. A search bar and sorting options are also present.

사이버아크 아이덴티티 보안 플랫폼이 적용된 클라우드 환경 업무 수행 사례

사용자의 업무 편의성 유지 및 보안성 향상



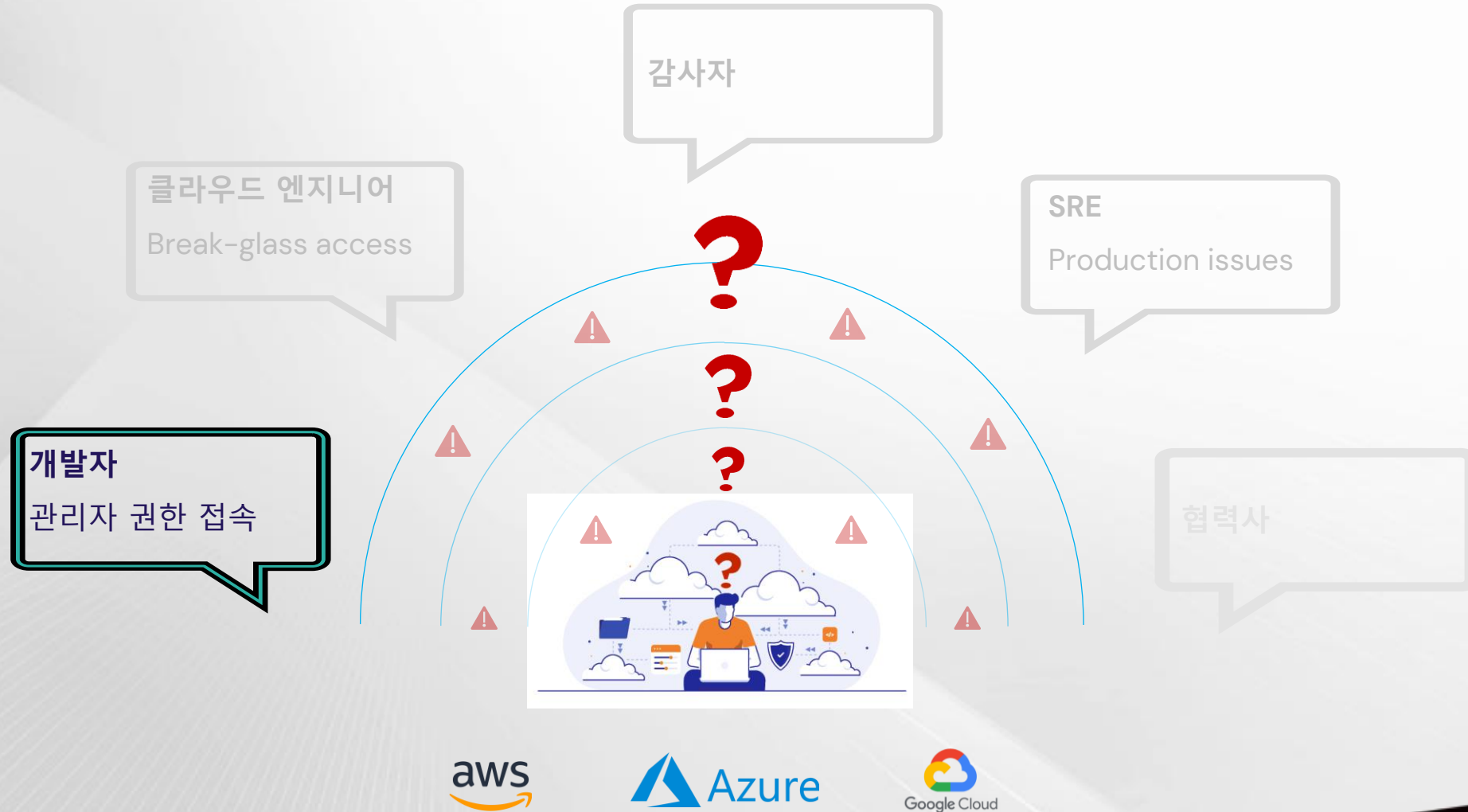
클라우드 보안 아키텍처

- 클라우드 접속에 대한 보안고민
 - 과도한 권한 접속을 통한 데이터 유출 위험 감소.
 - 고정 권한을 줄이고, 최소권한 원칙 구현
 - 사람 및 기계에 대한 클라우드 접속 정책 관리
 - 보안 상태와 규정 준수 유지
 - 클라우드 아이덴티티 활동에 대한 모니터링 및 감사



Messi
Cloud Security Architect

사용자 역할별 보안 적용



관리자 권한 접근

개발자
관리자 권한 접속

Access type: 매일 접속

What is important for her: 제한된 환경에서 신속한 업무 처리



Anat
클라우드 어플리케이션 개발자

클라우드 관리 및 인프라에 대한 안전한 접속



Messi
클라우드 보안 아키텍처



Anat
클라우드 어플리케이션 개발자

클라우드 관리 및 인프라에 대한 안전한 접속



제로 스탠딩 권한
(일시적 권한 부여)



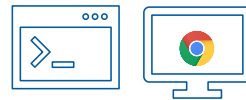
속성 기반 접근제어



최소 권한 접근



세션 모니터링 및 리코딩

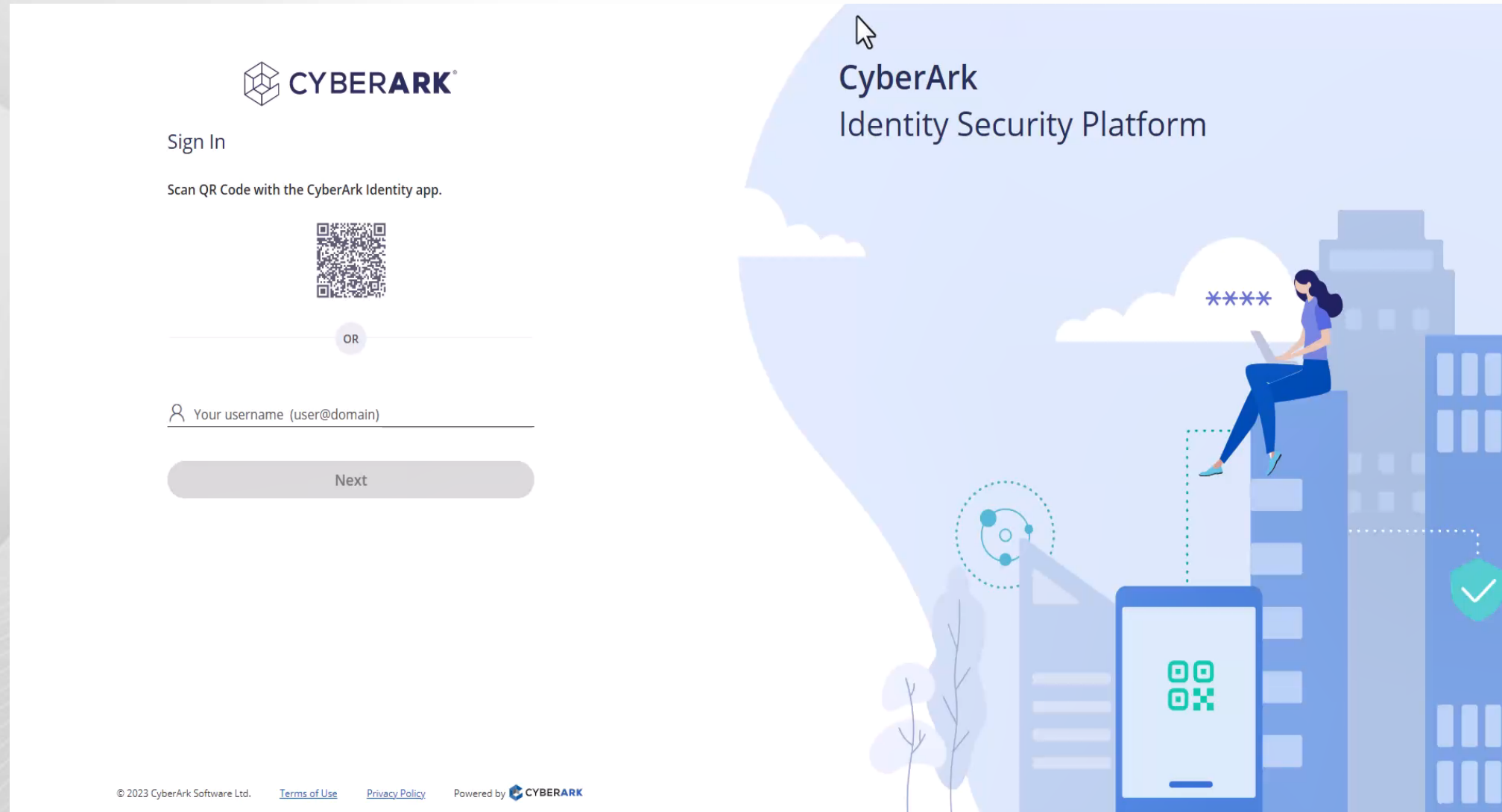



네이티브 접근 방식



세션 보호 및 이원화


보안 아키텍처의 정책 설정




 **CYBERARK**

Sign In


Scan QR Code with the CyberArk Identity app.



OR

 Your username (user@domain)

Next

© 2023 CyberArk Software Ltd. [Terms of Use](#) [Privacy Policy](#) Powered by  **CYBERARK**

CyberArk - Secure Cloud Access

se-pc-workshop.cyberark.cloud/securecloudaccess/policies

Incognito (2)

Messi

Access policies

Impact Project was registered with Secure Cloud Access

Status: All | Cloud provider: All | Policy type: All | Search

Create new policy

5 Policies

Policy	Status	Cloud provider	Entitlements	Created by	Last change	Description
Impact Project		Azure Resource	1	Messi	14/05/2023 07:52 PM	
AD roles		Azure AD	1	Top Gun	09/05/2023 09:18 AM	
Admin		IAM Identity center	1	Mike_Bykat	03/05/2023 11:01 PM	AWS Identity Center- SSO
Virtual Machine access		Azure Resource	4	Top Gun	27/04/2023 08:18 AM	
Read only and power admin		IAM Identity center	2	Top Gun	21/02/2023 10:53 AM	

Help

클라우드 관리 및 인프라에 대한 네이티브 접속

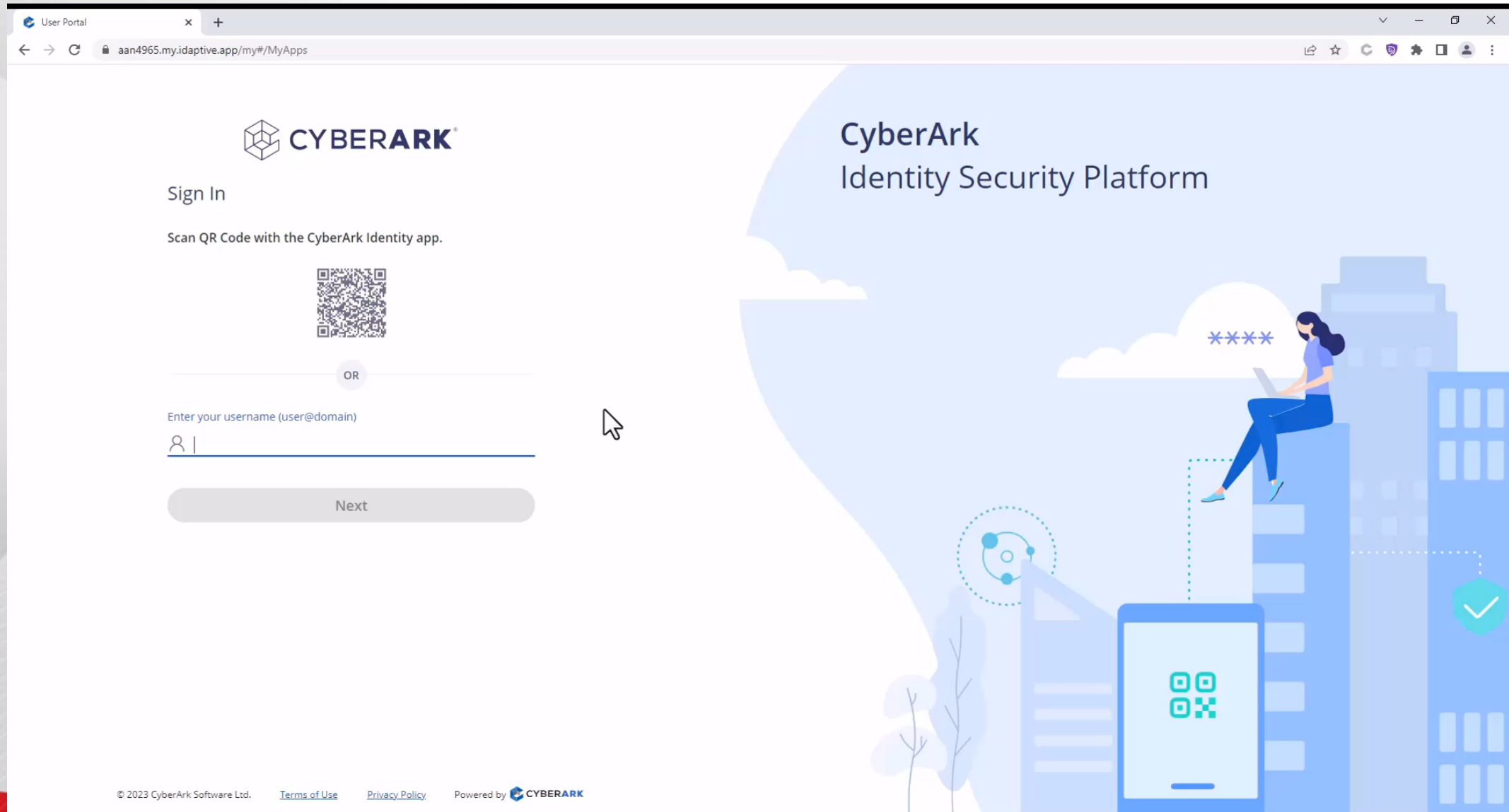


Messi
클라우드 보안 아키텍처



Anat
클라우드 어플리케이션 개발자

보안 적용에 따른 업무 수행




User Portal

aan4965.my.idaptive.app/my#/MyApps

CYBERARK®

Sign In

Scan QR Code with the CyberArk Identity app.



OR

Enter your username (user@domain)

Next

CyberArk
Identity Security Platform

© 2023 CyberArk Software Ltd. [Terms of Use](#) [Privacy Policy](#) Powered by **CYBERARK**

관리자 권한 접근

개발자
관리자 권한 접근

Access Type: 매일 접속

What is important for her: 제한된 환경에서 신속한 업무 처리

Method: JIT(Just In Time) 기반의 네이티브 접속

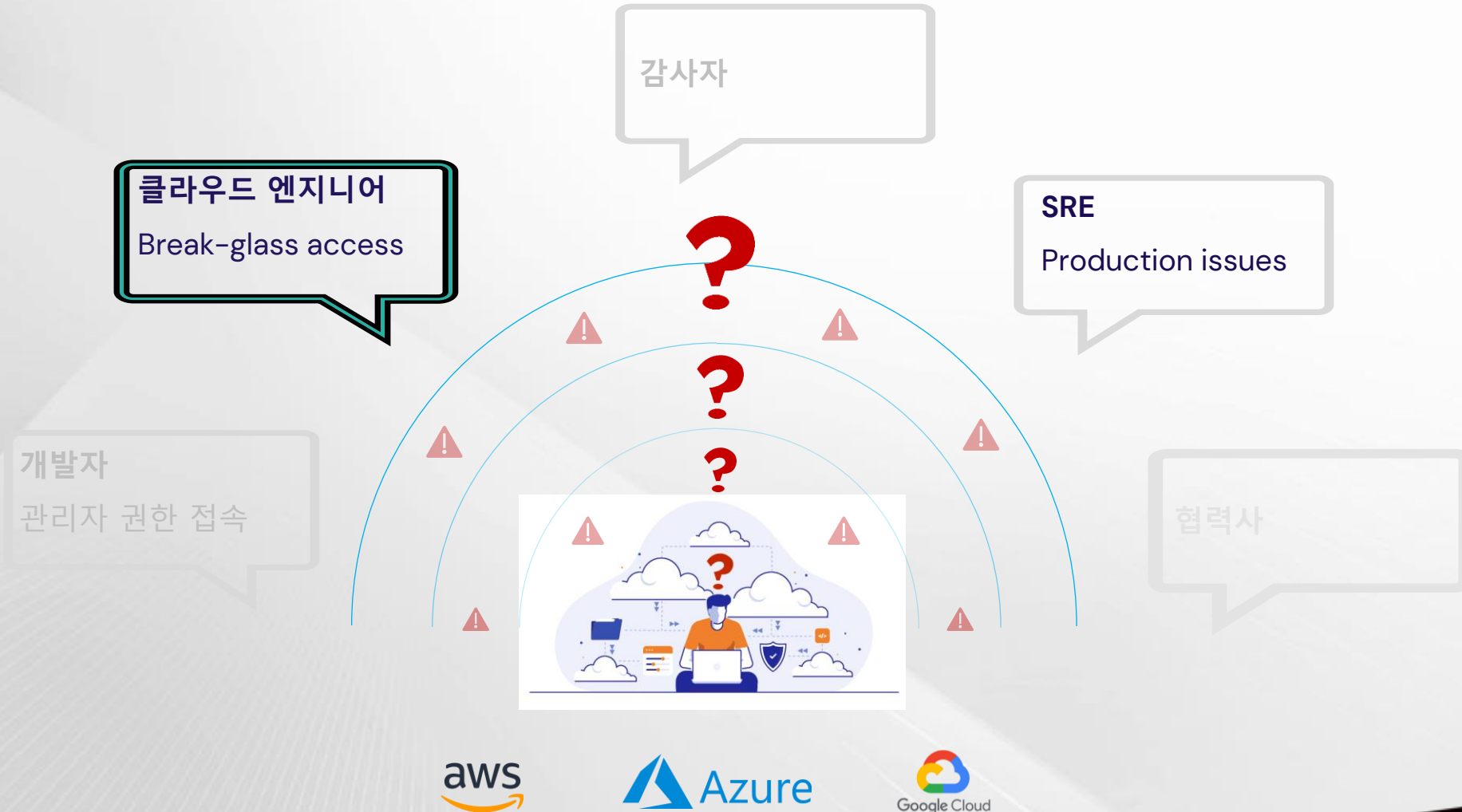
Benefits:

- ✓ 영구 권한 제거
- ✓ 최소 권한 접속
- ✓ 손쉬운 접근 (네이티브 접근 방식 제공)



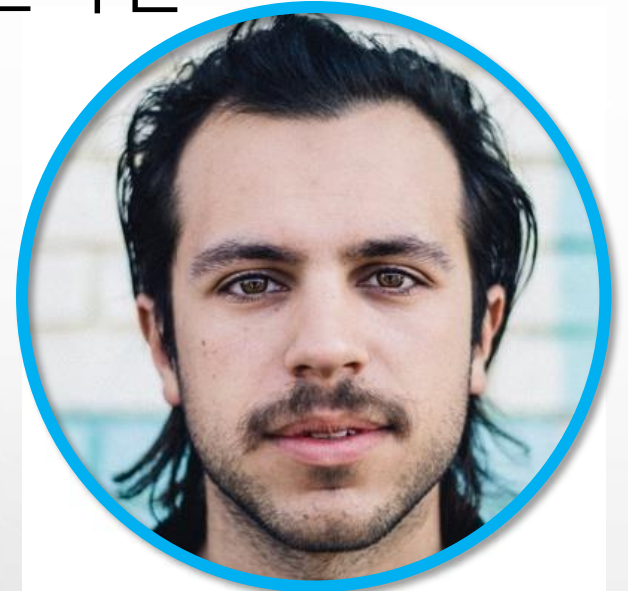
Anat
클라우드 어플리케이션 개발자

사용자 역할별 보안 적용



Break-glass

- **Access type:** 비상 상황에 따른 접근
- **What is important for him:** 제한된 환경에서 신속한 업무 처리
- **Method:** 관리자 계정에 대한 중앙 관리
- **Benefits:**
 - ✓ 관리 및 감사 추적 제공



Mike
클라우드 엔지니어

운영 환경 관리(이슈 해결)

SRE

Production issues

Access type: 필요시 마다 접근

What is important for him: 신속한 접근 권한 획득

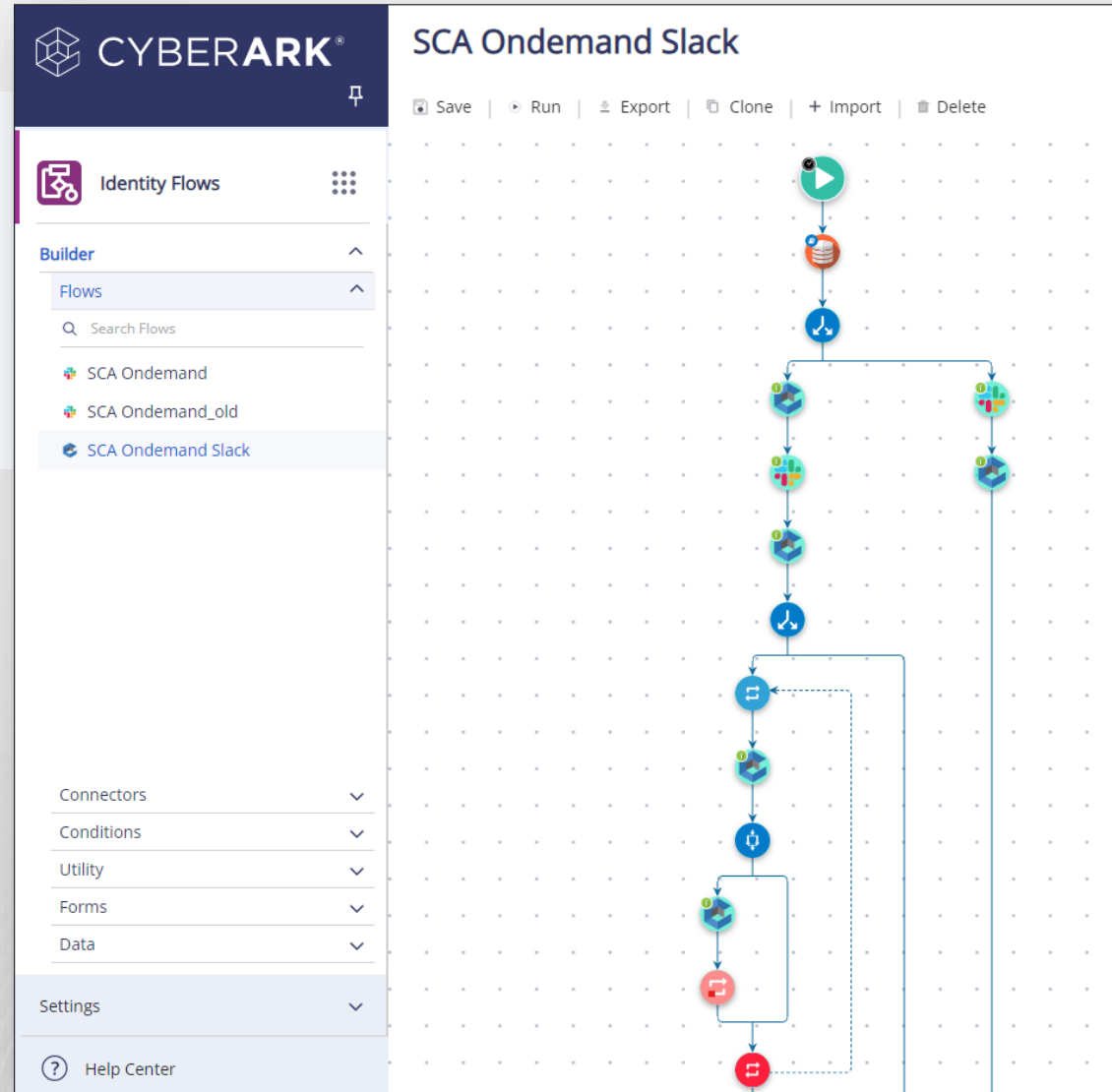


Joe
SRE

셀프 서비스 접근 요청

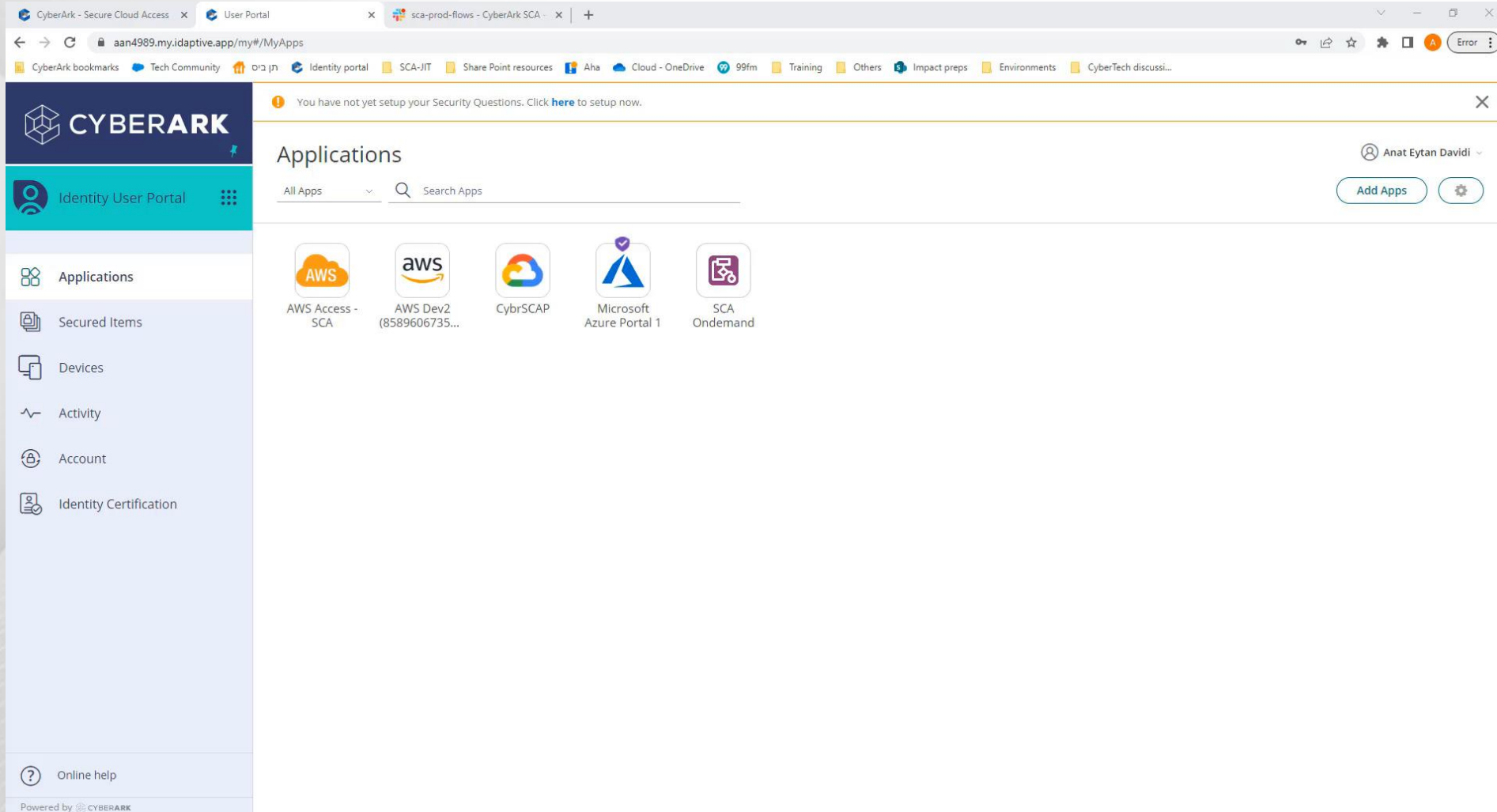


셀프 서비스



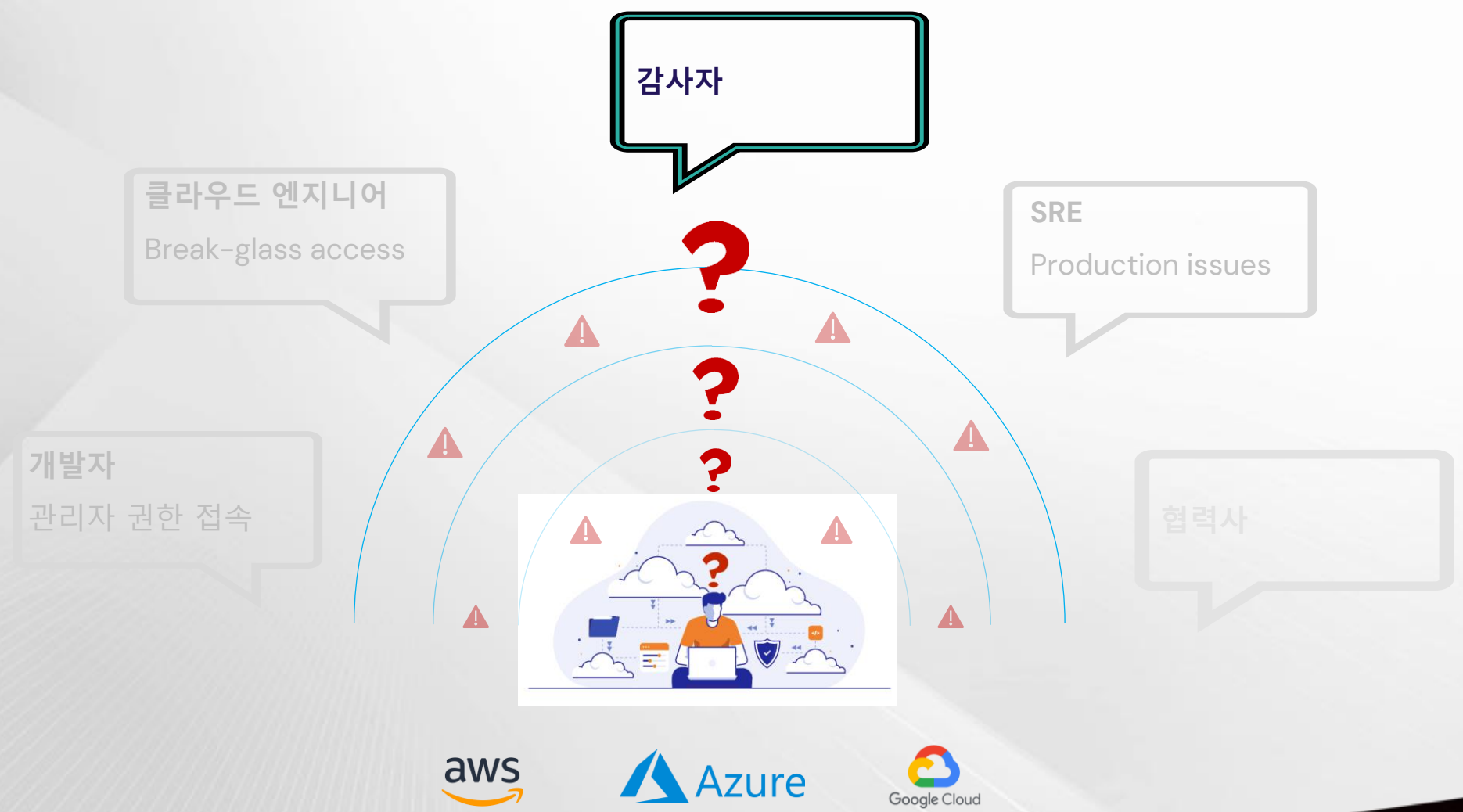
링 시스템 및 Slack과 Chatops 도구와

보안 적용에 따른 업무 수행



The screenshot shows the CyberArk Identity User Portal interface. At the top, there is a navigation bar with the CyberArk logo and a user profile for Anat Eytan Davidi. Below the navigation bar, the main content area is titled "Applications" and features a search bar and an "Add Apps" button. The main content area displays a grid of application tiles, each with an icon and a label: "AWS Access - SCA", "AWS Dev2 (8589606735...)", "CybrSCAP", "Microsoft Azure Portal 1", and "SCA Ondemand". On the left side, there is a sidebar with a menu containing "Applications", "Secured Items", "Devices", "Activity", "Account", and "Identity Certification". At the bottom of the sidebar, there is an "Online help" link and a "Powered by CYBERARK" logo.

사용자 역할별 다른 접근 방식



감사자

감사자

- **What is important for her:**

- 필요한 로그 및 이벤트를 신속하게 검색
- 감사 및 규정 준수 요구에 대한 만족
- 누가 어떤 리소스에 접근하고 무엇을 했는지에 대한 추적



Karen
Auditor

모든 업무 행위에 대한 감사

Microsoft Azure portal interface showing session recording details. The top bar includes 'Step Recording', 'Continuous Authentication', and 'Session Protection'. A timeline on the left lists 11 steps for May 01, 2023, such as 'Mouse clicked Roles' and 'Role assignments'. The main content area shows the 'Access control (IAM)' page for a specific resource group.

Cloud Monitoring dashboard showing 'Events over Time' for 'Operation Type: Create'. The chart displays activity from Sep 05, 8 AM to Sep 06, 8 AM, with a callout for '2 Anomalous Activities' (Temporary Token Chaining and Unusual Activity). Below the chart is a table of events:

Cloud	Event Name	Event Time	Status	Identity Name	Identity Type	Resource	Source IP	Operation Type	Actions
aws	CreateUser	2022-09-06 07:52:53	✓	ajay.acme.com	Federated User	app-user	104.24.10.55	Create	...
aws	CreateBucket	2022-09-06 07:37:23	✓	ajay.acme.com	Federated User	dm-dept-storage	104.24.10.55	Create	...
aws	CreateAccessKey	2022-09-06 06:45:39	✗	dmuser	User	monitor-user	105.25.1.35	Create	...
	v1.compute.Instance.Create	2022-09-06 06:22:45	✗	cm-func-acct@acme.iam.iam.gserviceaccount.com	Service Account	-	105.26.4.56	Create	...
aws	RunInstances	2022-09-06 05:32:63	✓	cyana@acme.com	Federated User	i-0852e084d4017e041	105.28.4.103	Create	...
	v1.compute.Instance.Create	2022-09-06 04:44:23	✗	cm-func-acct@acme.iam.iam.gserviceaccount.com	Service Account	-	104.26.7.106	Create	...
	v1.iam.ServiceAccounts.create	2022-09-06 04:21:54	✗	john.doe@acme.com	Federated User	co-staging-acct@acme.iam.gserviceaccount.com	105.34.5.58	Create	...
aws	AssumeRole	2022-09-06 03:56:24	✗	rm_user	User	rm-dpg-role	104.23.4.108	Create	...
	v1.storage.objects.create	2022-09-06 03:16:34	✓	cyana@acme.com	Federated User	bucket-staging-dept	104.25.3.59	Create	...

• Benefits:

✓ 멀티 클라우드 환경에 대한 통합 감사

통합 위협 분석 포탈 제공

- 사용자 이상행위, 권한 남용 등에 대한 탐지/조사 및 대응



비정상적이고 위험한 상황에 대한 통합 탐지 및 예방:

- SSO/MFA를 통한 웹 어플리케이션 접속
- 사이버아크 SaaS 기반 PAM 솔루션에서의 위험 행위 탐지(명령어 위반, 비정상 접속 행위 등)

주요 제공 기능:

- 사용자 행위에 대한 통찰력과 포괄적인 위험 점수를 갖춘 통합 UI
- SIEM 솔루션과의 연계
- 감사, 규정 준수 및 포렌식을 위한 검토 가속화를 위한 위험 점수화
- 자동화 및 권장 대응 조치 실행

To Summarize

96%

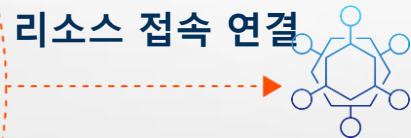
보안 결정권자 중 96%는 제로 트러스트가 자신들의 성공에 중요하다고 언급



리소스 접속 요청



Machine



Enterprise Resource

리소스 접속 연결

76%

보안 결정권자 중 76%가 구현 과정에 있다고 언급

사이버아크는 강력한 적응형 인증, 지속적인 승인 및 인가, 최소한의 권한 액세스, 자격 증명 및 인증 보호, 그리고 지속적인 모니터링 및 인증을 포함한 핵심 아이덴티티 기반 보안 원칙을 구현함으로써 기업들이 고민하는 제로 트러스트 기반의 통합 클라우드 환경 보안을 제공합니다



CYBERARK[®]
The Identity Security Company

김광수 부장

+82-10-6556-0120

Kwangsoo.kim@cyberark.com