



CYBERARK®
The Identity Security Company™

차세대 시스템접근제어 PAM

사이버아크 코리아

cyberark.is/identity-security



Who Are We

사이버아크는 아이덴티티 신원보안 분야의 글로벌 선두주자
입니다. **비즈니스 애플리케이션, 분산된 업무 인력,
하이브리드 클라우드 워크 로드 및 데브옵스 라이프사이클
전반에 걸친** 모든 신원(Human, Non-Human)에 대한 가장
포괄적인 보안 솔루션을 제공합니다.



1999년도 설립
이스라엘 및 뉴튼,
매사추세츠(미국) 본사

>8,500
1,400
110

글로벌 8,500개 고객사
1,400 비즈니스 파트너
110개 국가 영업 중



3,000명 이상 임직원

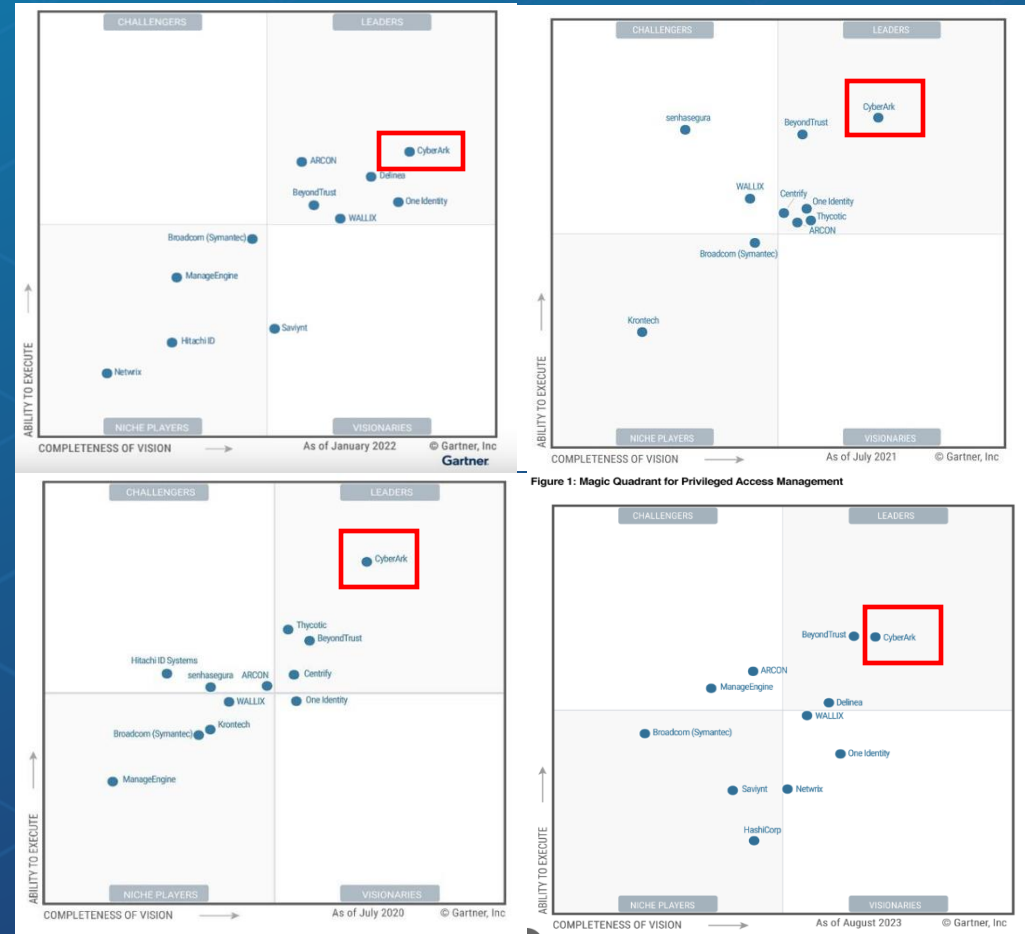


하이브리드, 멀티
클라우드 환경의 사용자
및 비-사용자형
아이덴티티 보안을
제공하는 유일한 벤더

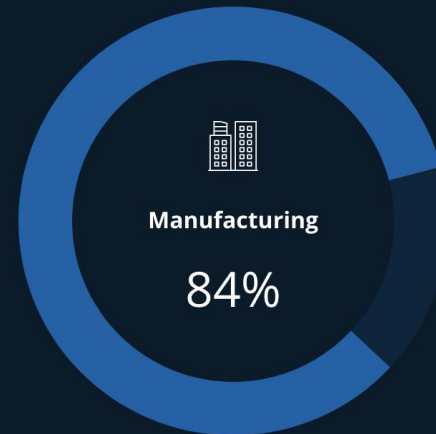
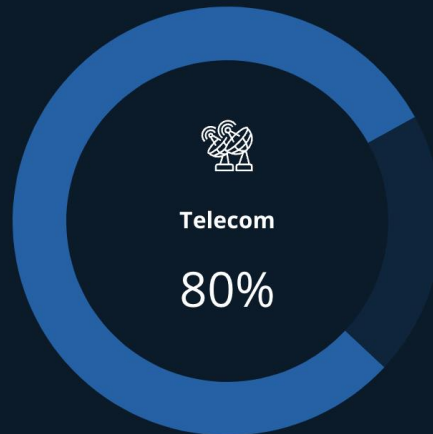
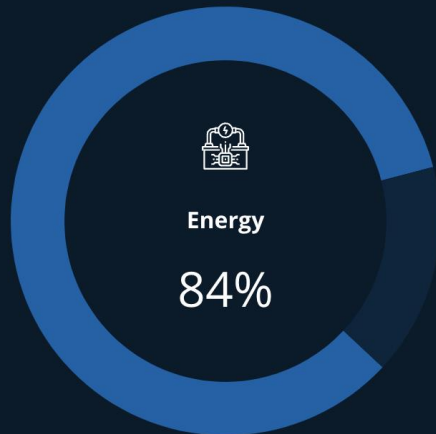
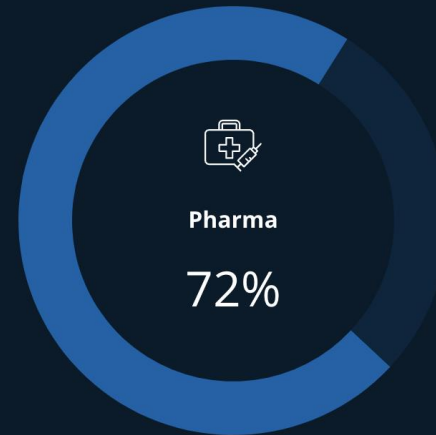
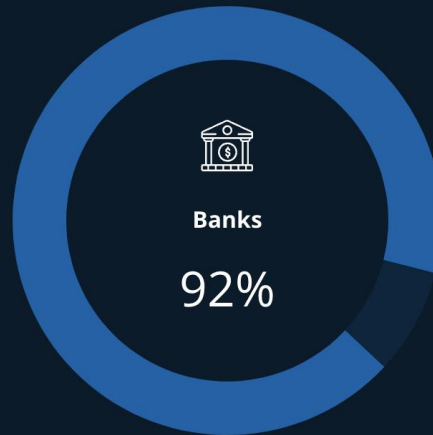
가트너 선정 차세대 시스템접근제어 PAM 리더

사이버아크 솔루션은 차세대 시스템접근제어 PAM 분야에 가장 높은 능력을 인정 받고 있습니다.

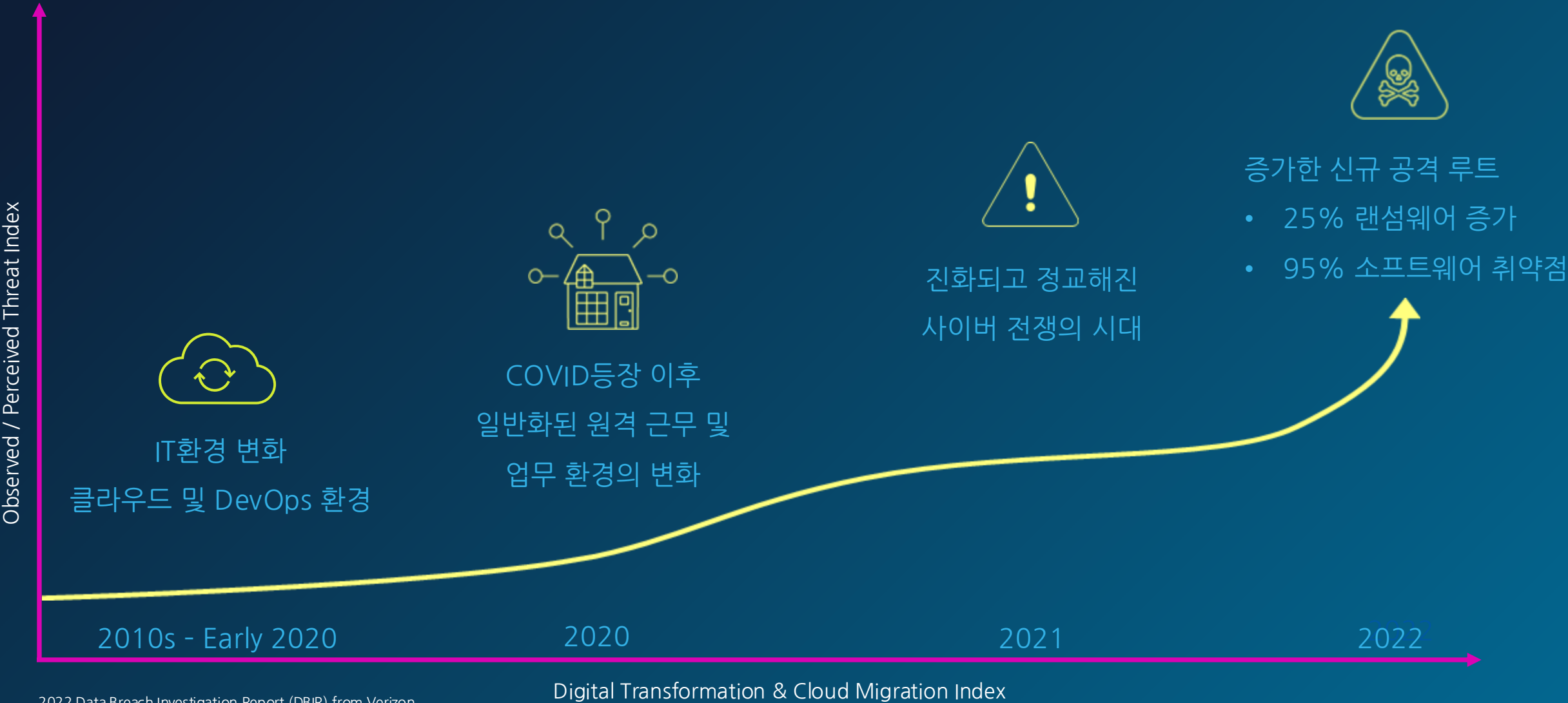
Figure 1: Magic Quadrant for Privileged Access Management



글로벌 Top 500대 기업은 사이버아크 선택

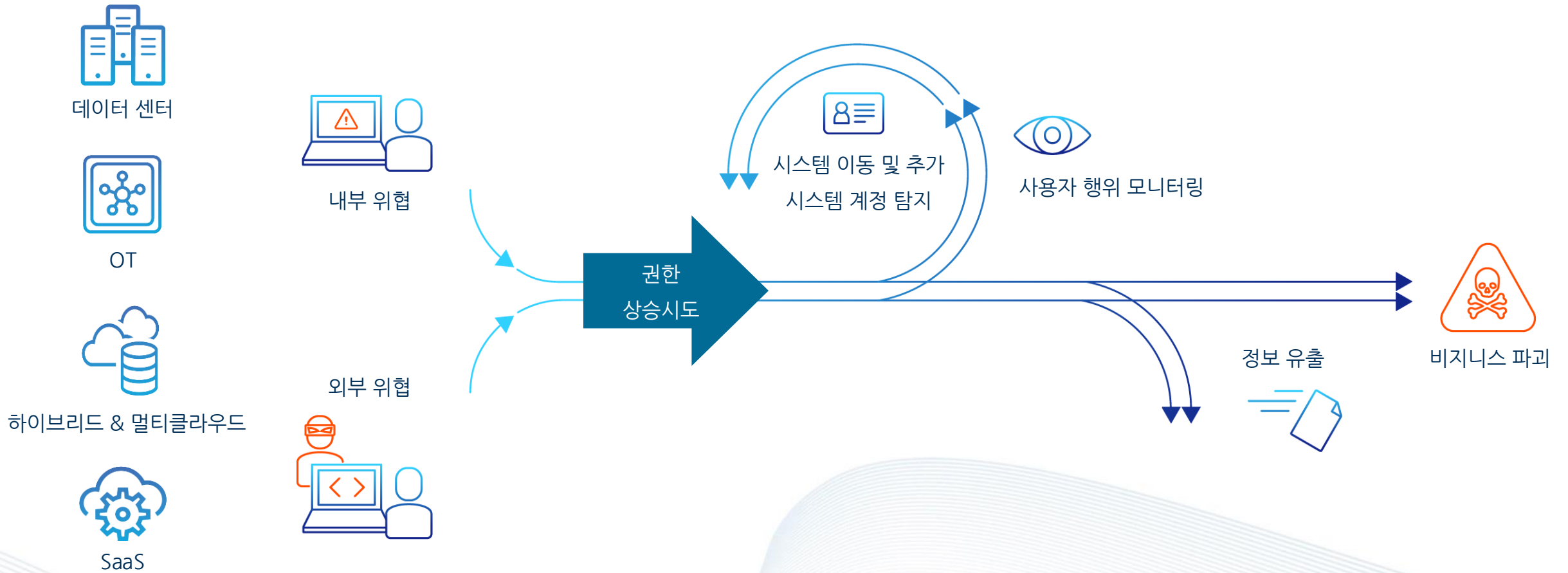


진화하는 사이버공격 기법

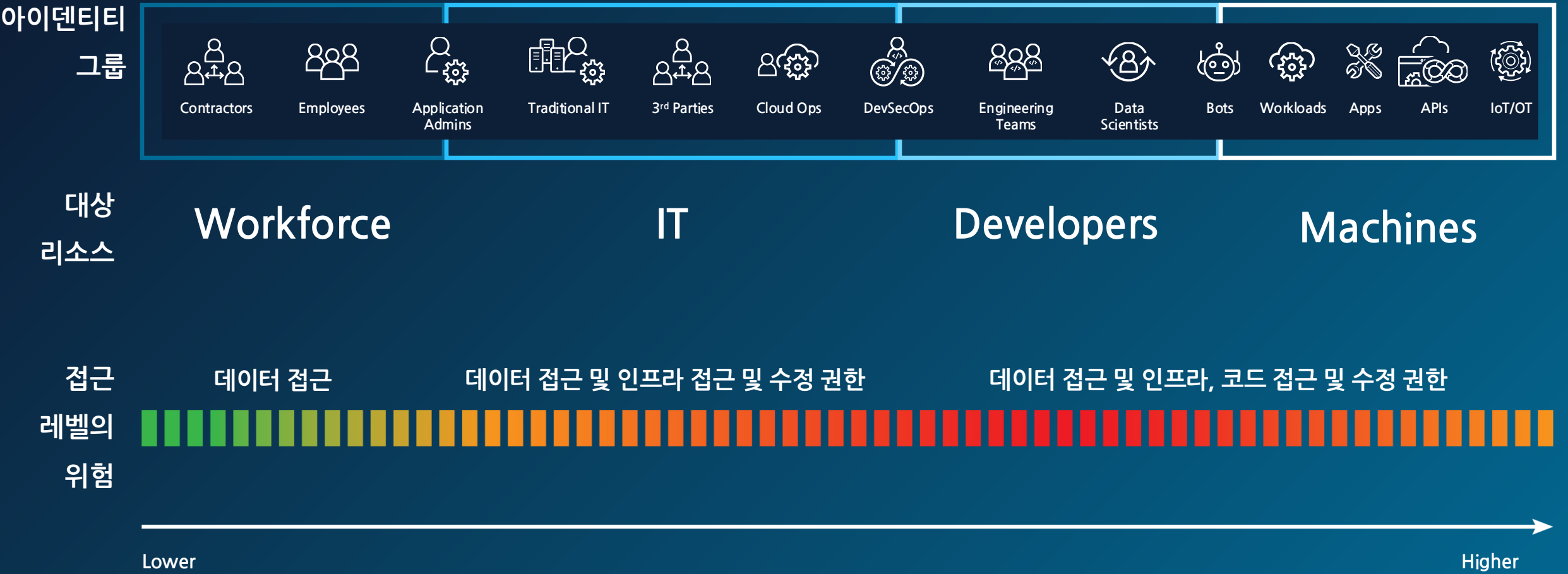


2022 Data Breach Investigation Report (DBIR) from Verizon

여전히 가장 파괴적인 공격기법



다양한 아이덴티티 유형



모든 아이덴티티 보안을 위한 솔루션



Workforce



IT



Developer



Machines

IDENTITY SECURITY

일반 사용자 보안

높은 권한의 일반 사용자 보안

IT 관리자 보안

클라우드 운영 보안

개발자, DevOps 보안

워크로드 아이덴티티 보안

하이브리드 환경 보안

Secure Desktops & Servers



CYBERARK®

Identity Security Platform



다양한 유형의
아이덴티티

Workforce

일반 사용자 보안
높은 권한의 일반
사용자 보안

IT

IT 관리자 보안
클라우드 운영 보안

Developers

개발자
DevOps 보안

Machines

워크로드
아이덴티티 보안
하이브리드 환경
보안

제로 트러스트 기반 접근제어

접근 대상

상시 사용

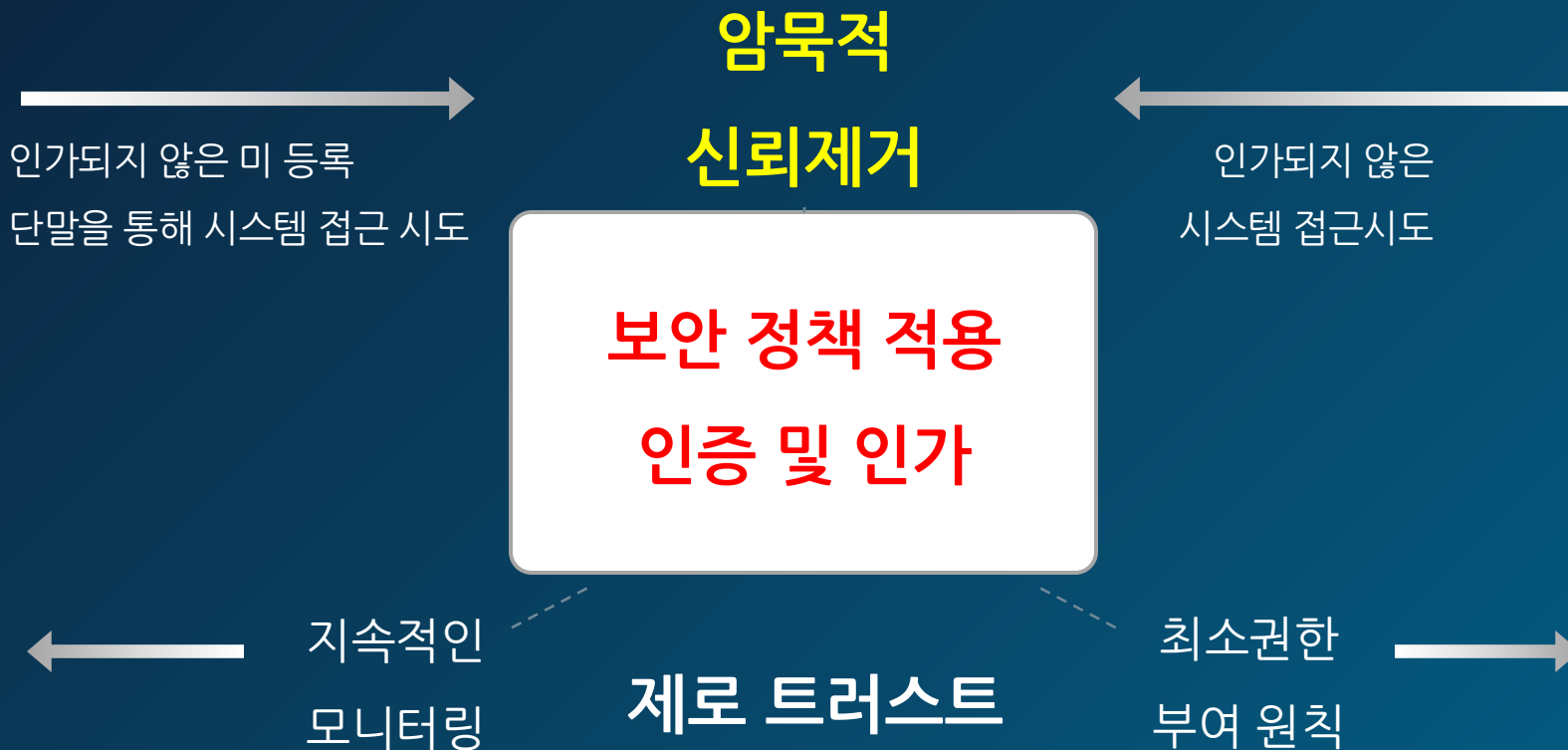
엔드포인트
데이터
SaaS 애플리케이션

고 위험 환경

데이터센터
워크로드
CI/CD 툴

멀티클라우드 콘솔
클라우드 서비스
클라우드 워크로드
Code Repos

대상 리소스 자동화 툴



다양한 유형의 아이덴티티

접근 대상

Workforce

일반 사용자 보안
높은 권한의 일반
사용자 보안

IT

IT 관리자 보안
클라우드 운영 보안

Developers

개발자
DevOps 보안

Machines

워크로드
아이덴티티 보안
하이브리드 환경
보안

상시 사용

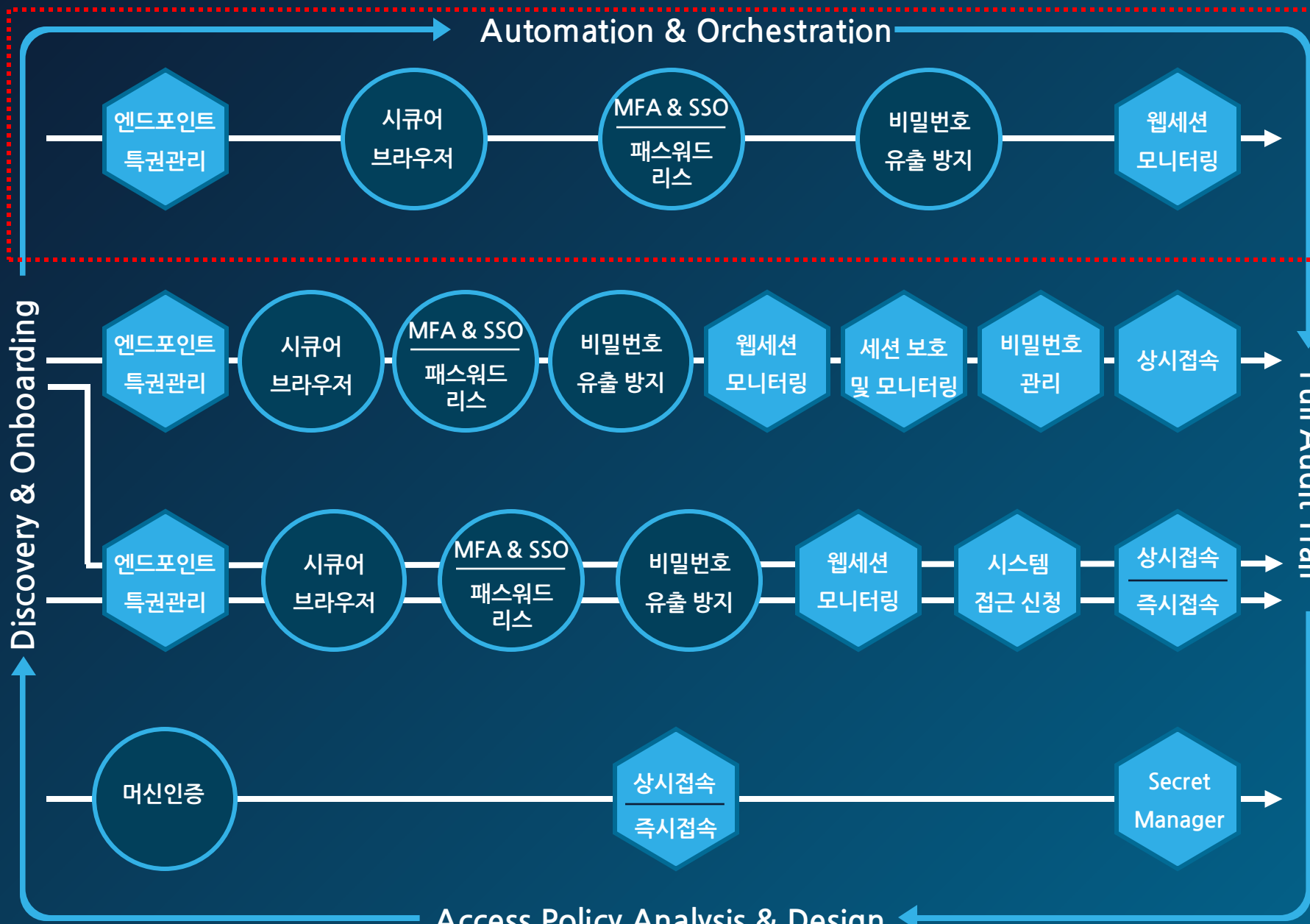
엔드포인트
데이터
SaaS 애플리케이션

고 위험 환경

데이터센터
워크로드
CI/CD 툴

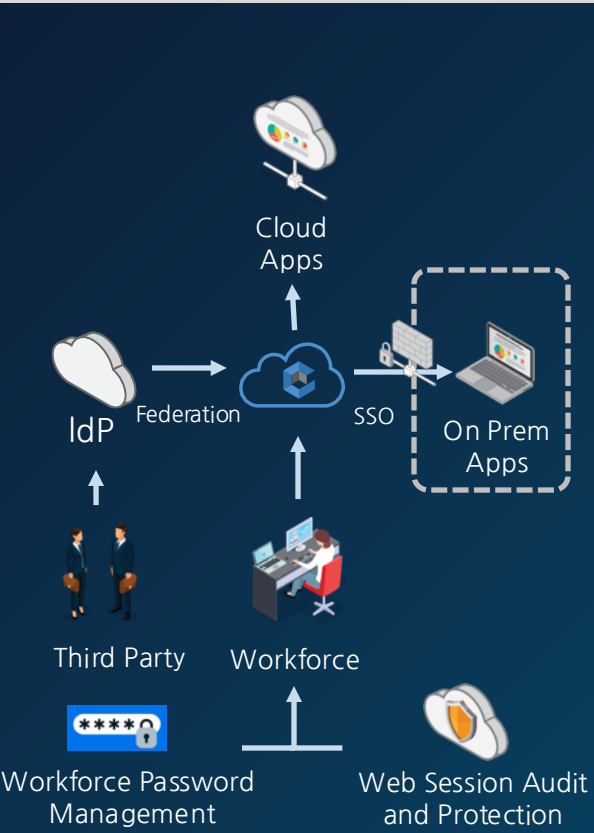
멀티클라우드 콘솔
클라우드 서비스
클라우드 워크로드
Code Repos

대상 리소스 자동화 툴

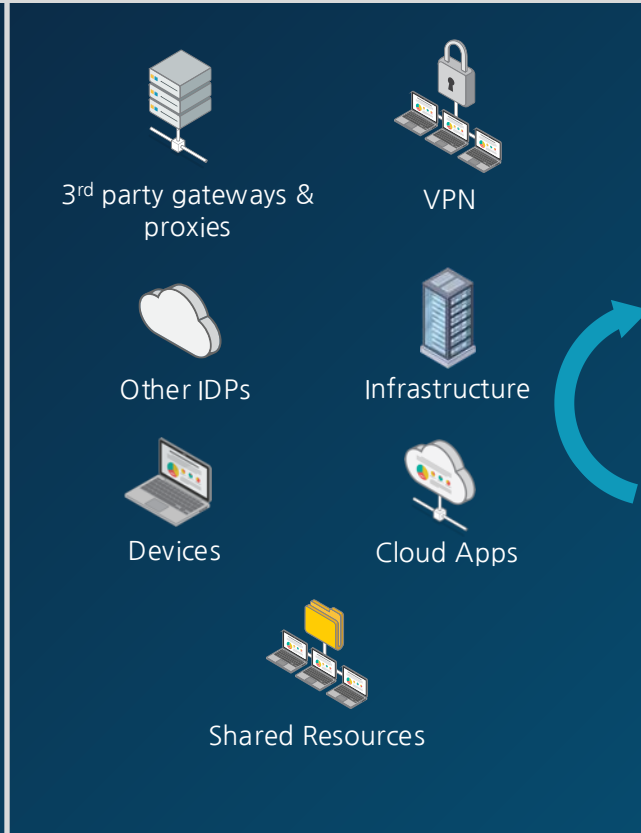


주요 기능# 사용자 통합 인증

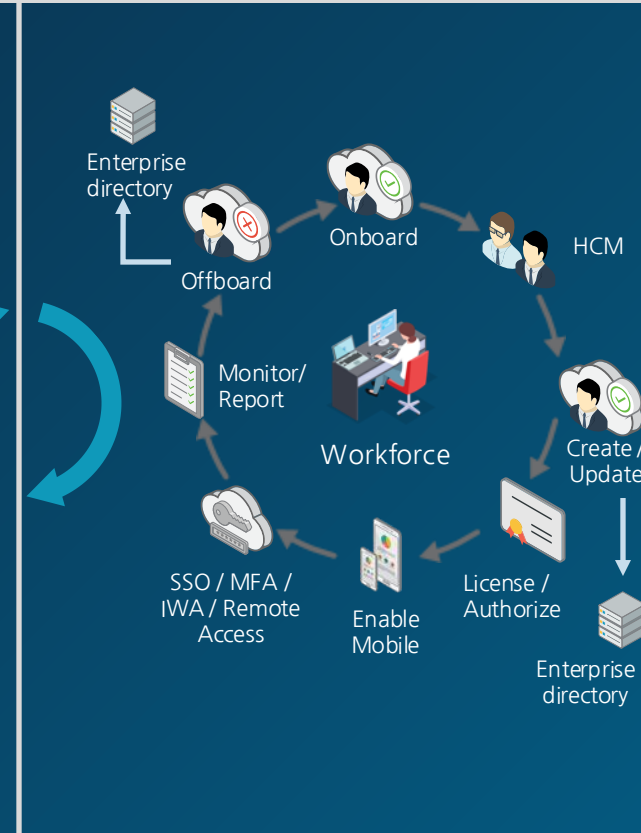
SSO포탈



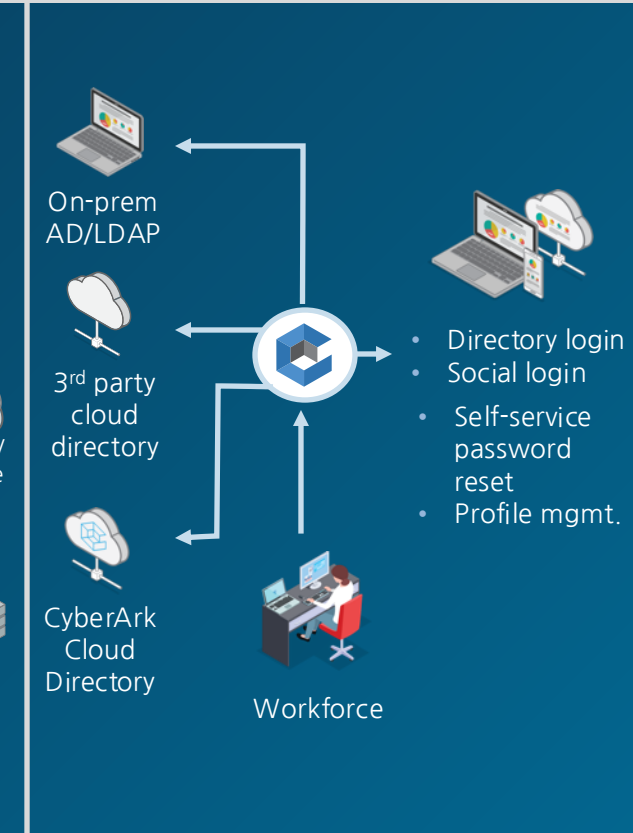
MFA



계정 라이프사이클 관리

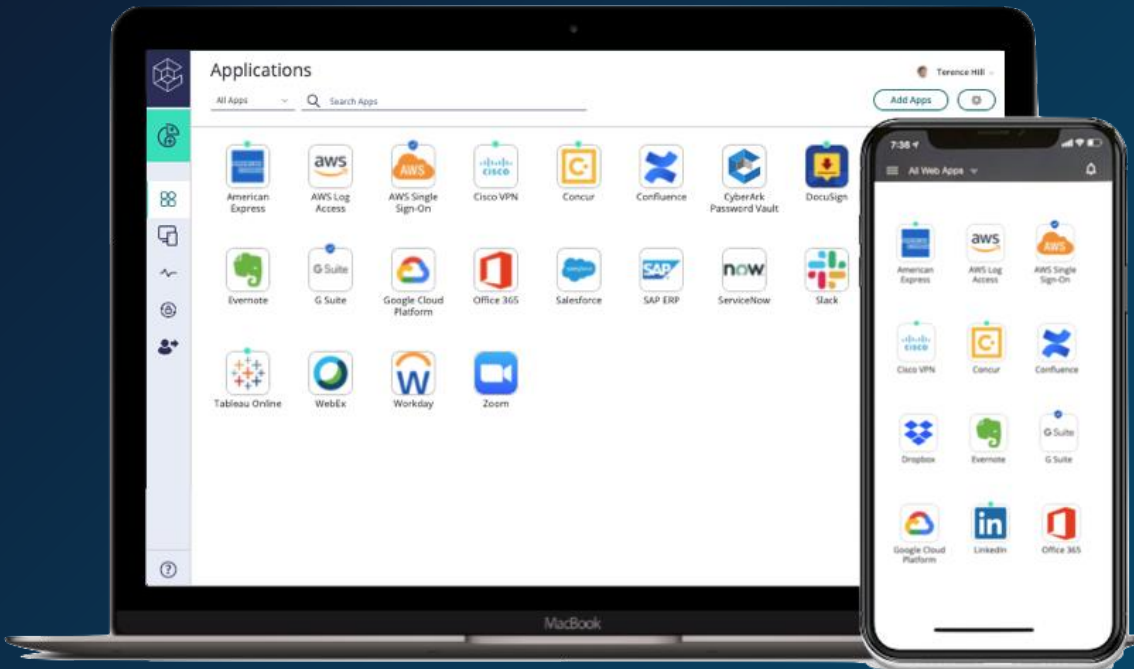


디렉토리 연계



주요 기능# 웹 애플리케이션 SSO

사용자 업무 향상, 헬프 데스크 업무 부하 감소 및 컴플라이언스 준수 제공



한번의 클릭으로 회사 업무 접속

클라우드 및 레가시 앱 사용

SSO

SSO 표준을 활용하는 모든
클라우드 및 온프레미스 앱에
단일 로그인

App Catalog

이미 연동되어 있는 수천개의 웹
업무 및 모바일 앱에 대한
손쉬운 SSO 구성

Self-Service Password Reset

사용자들의 패스워드 변경 및
계정 잠금 해제 등을 위한 셀프
서비스

VPN-Less App Access

온프레미스 앱에 대한 VPN-less
방식 액세스

주요 기능# 다양한 MFA요소 제공

인증 강화 및 사용자의 편의성을 위해 다양한 형태의 이중인증 수단 제공

Authentication Profile

Profile Name *
Marketing User Portal Login Minimum AAL: ● AAL2 Maximum AAL: ●●● AAL3

Multiple Authentication Mechanisms

Challenge 1

Something you have

- ☐ Mobile Authenticator
- ☐ Phone call
- ☐ OATH OTP Client
- ☐ Text message (SMS) confirmation code
- ☐ Duo
- ☐ Email confirmation code
- ☐ QR Code
- ☐ FIDO2 Authenticator(s) (single-factor)

Something you are

- ☐ FIDO2 Authenticator(s) (multi-factor)

Something you know

- ☒ Password
- ☐ Security Question(s)
1 Number of questions user must answer

Other

- ☐ 3rd Party RADIUS Authentication

Challenge 2 (optional)

Something you have

- ☒ Mobile Authenticator
- ☐ Phone call
- ☐ OATH OTP Client
- ☐ Text message (SMS) confirmation code
- ☐ Duo
- ☐ Email confirmation code
- ☐ QR Code
- ☒ FIDO2 Authenticator(s) (single-factor)

Something you are

- ☐ FIDO2 Authenticator(s) (multi-factor)

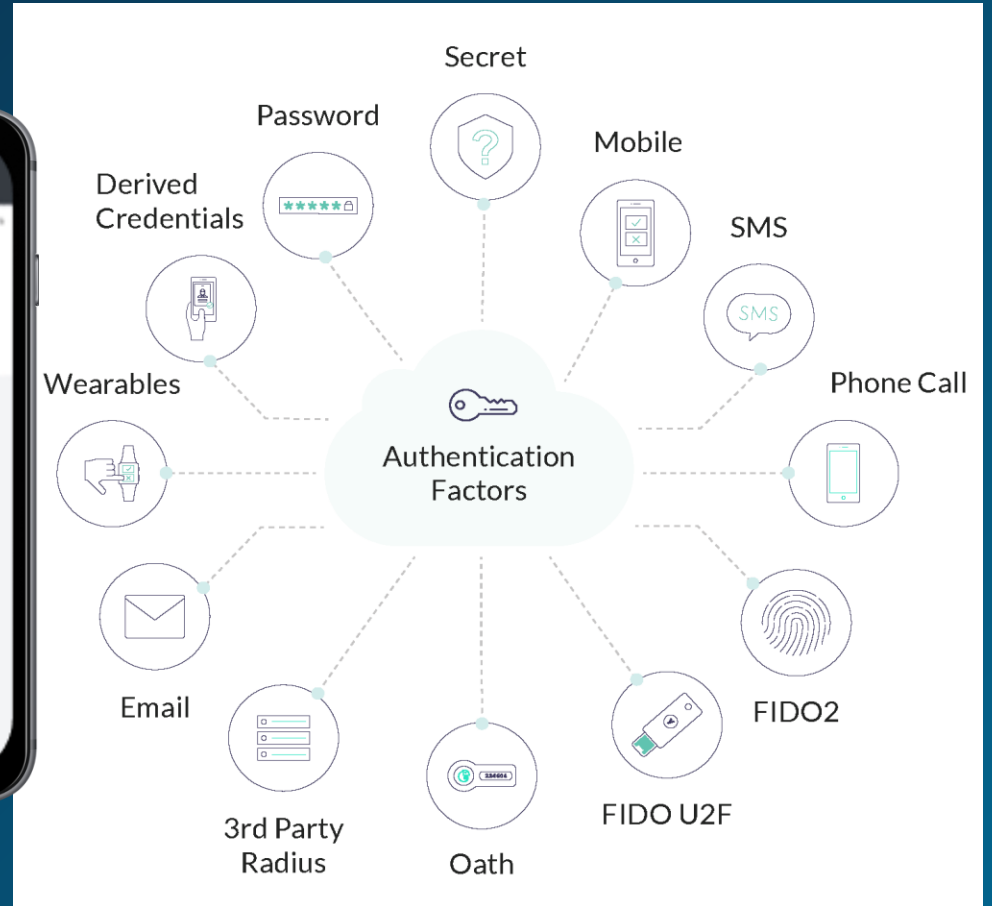
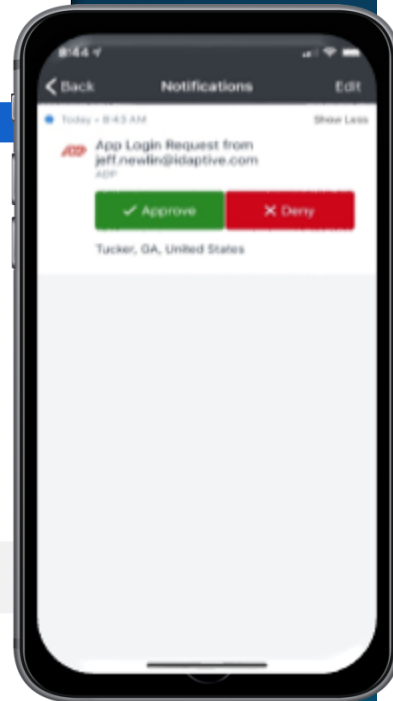
Something you know

- ☐ Password
- ☐ Security Question(s)

Other

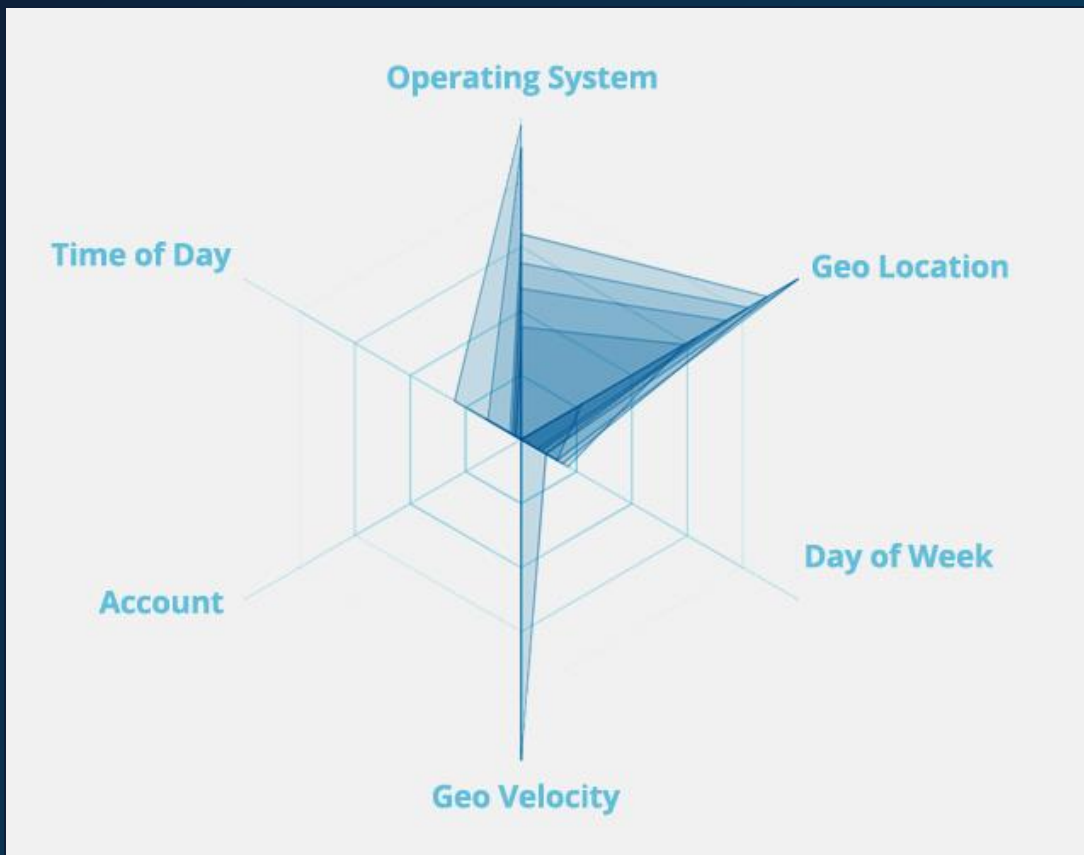
- ☐ 3rd Party RADIUS Authentication

OK Cancel



주요 기능# 적응형 MFA

환경 변화에 따라 차등 된 MFA요소를 적용하여 강력한 보안 제공



유저 환경 변화 자동탐지

액세스 유저 환경에 대한 차등 된 MFA적용

MFA Everywhere

액세스 시간, 단말, IP, 브라우저, OS버전, 국가 등 환경 변화 탐지

Board Authentication

SMS, App, Email, Phone Call 등. 다양한 형태의 인증 수단

보안 위협 탐지

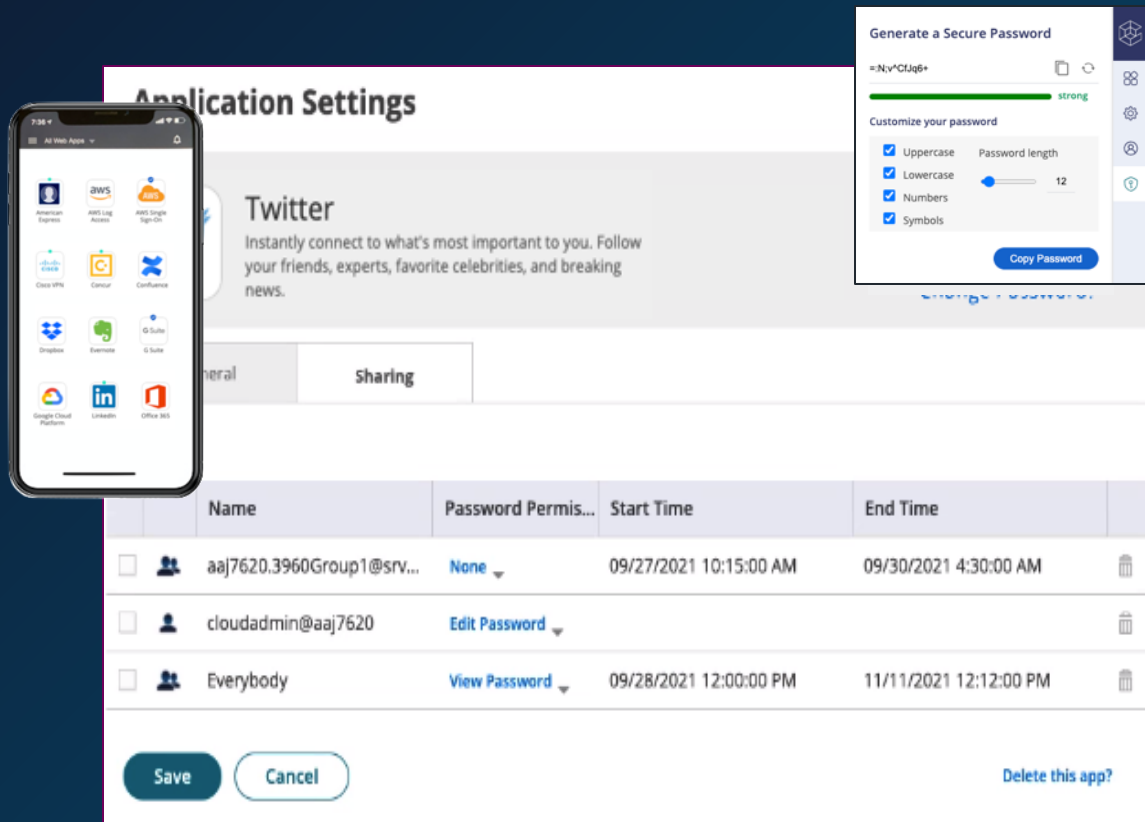
사용자 인증 행위에 대한 머신러닝 기법의 위협 분석 제공

VPN-Less App Access

Oath, FIDO, Radius 등 다양한 표준 프로토콜을 통한 연계 제공

주요 기능# 브라우저 캐시 보안 WPM

기업 및 사용자 개인 애플리케이션 비밀번호를 안전하게 저장



웹 애플리케이션 비밀번호 관리

클라우드 또는 구축형 Vault 서버에 저장

비밀번호 중앙관리

IDP와 연동하여 보안정책을 정의 및 하고 보안 및 규정 준수 보고서 통합

안전한 접근제어

자체 호스팅된 스토리지 또는 클라우드에 비밀번호 저장

안전한 비밀번호 공유

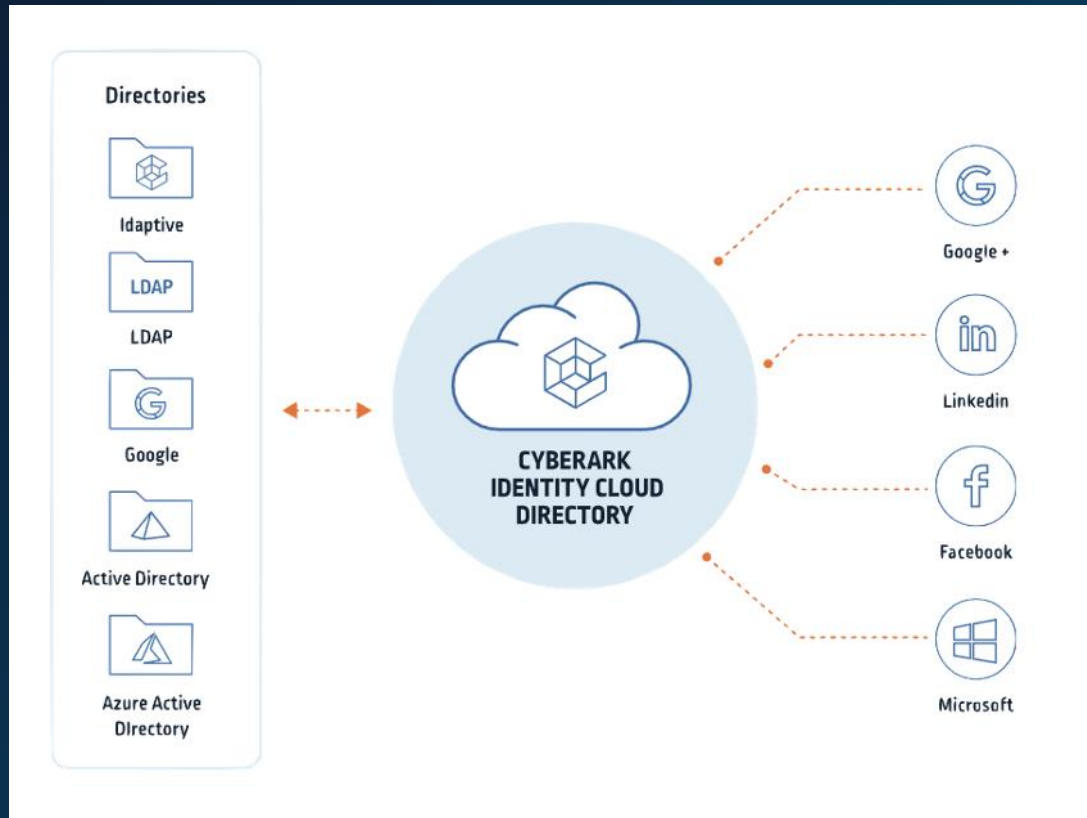
인가된 사용자와 안전한 채널을 통해 비밀번호 공유

리포팅 및 가시성

유저 활동 기록을 모니터링 하고, 암호 복잡성을 제어

주요 기능# 디렉토리 서비스

차세대 시스템접근제어에 대한 별도 라이선스 없이 무료 제공



온프레미스 및 클라우드 환경 디렉토리 통합

계정 정보에 대한 통합

비밀번호 중앙관리

IDP와 연동하여 보안정책을
정의 및 하고 보안 및 규정 준수
보고서 통합

안전한 접근제어

자체 호스팅된 스토리지 또는
클라우드에 비밀번호 저장

안전한 비밀번호 공유

인가된 사용자와 안전한 채널을
통해 비밀번호 공유

리포팅 및 가시성

유저 활동 기록을 모니터링 하고,
암호 복잡성을 제어

주요 기능# Trust Agent

Agent 설치된 인가된 단말을 통해 SSO포탈 접속 허용

 **CYBERARK**

 Identity Administration

 Access Orchestrator

 Apps & Widgets

Web Apps

Widgets

 Downloads

 Settings

Customization

CyberArk Identity Downloads

Download additional software for extending CyberArk Identity into your environment.

All  Search all downloads

	Name	Service		Version	
▼	Agents				
	Windows Cloud Agent	Endpoint Services			 Download
	Mac Cloud Agent	Endpoint Services			 Download
	Mac Device Trust Agent	Endpoint Services			 Download
	Windows Device Trust	Endpoint Services			 Download
▼	Browser Extensions				
	Chrome	Application Services		23.8.219	 Download

주요 기능# 모든 세션 제어 및 모니터링

대상 시스템 접근 세션에 대한 모니터링 및 감사



ISOLATE

사용자로부터 대상 시스템으로의
직접적인 접근 차단



MONITOR

이상 행위 탐지 및 실시간 이벤트
생성을 통한 모니터링 및 추적 제공



RECORD

모든 행위 상세 감사 및 포렌시 분석 제공
(동영상 재생 및 입력 명령어의 텍스트
기반 기록)

주요 기능# 모든 세션 제어 및 모니터링

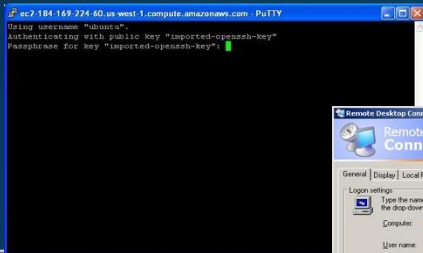
원격접속 사용자의 모든 세션은 타겟 업무시스템과 이원화 시키고, 모든 내역을 모니터링



접속 계정 탈취 차단 및 모든 세션 감사



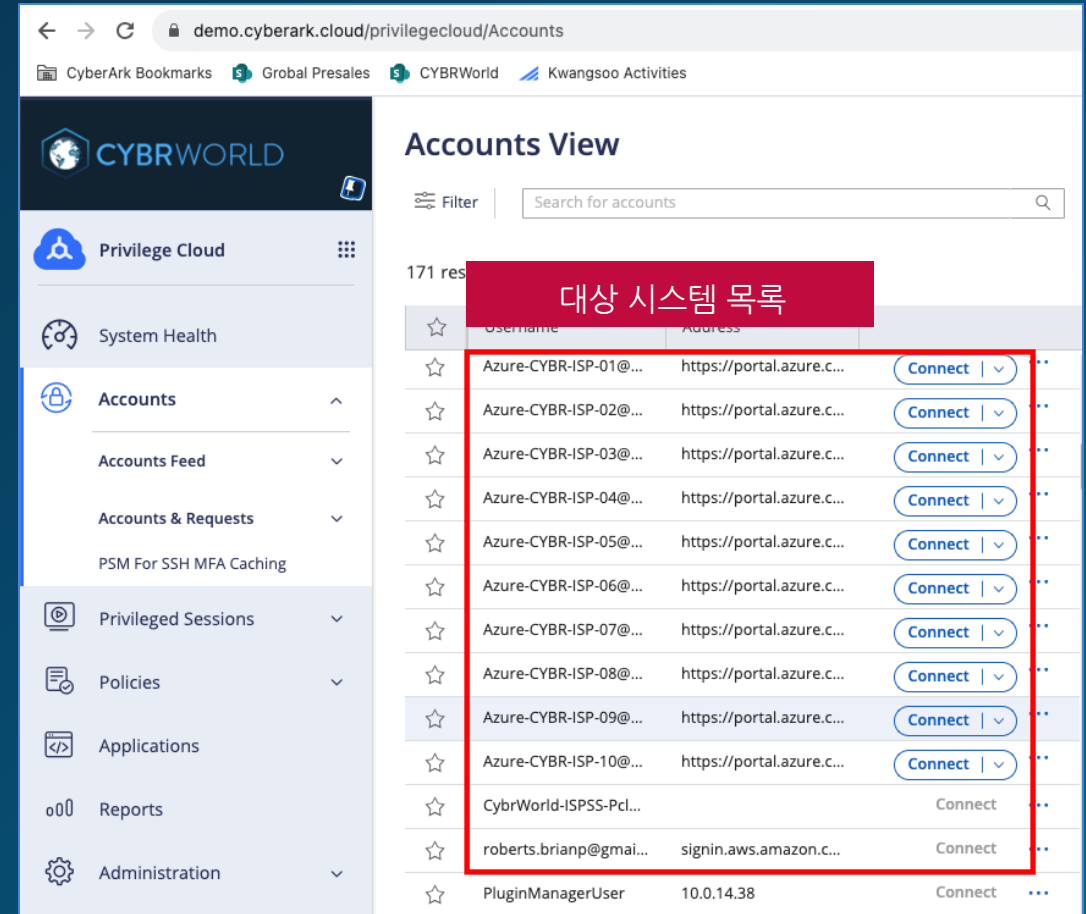
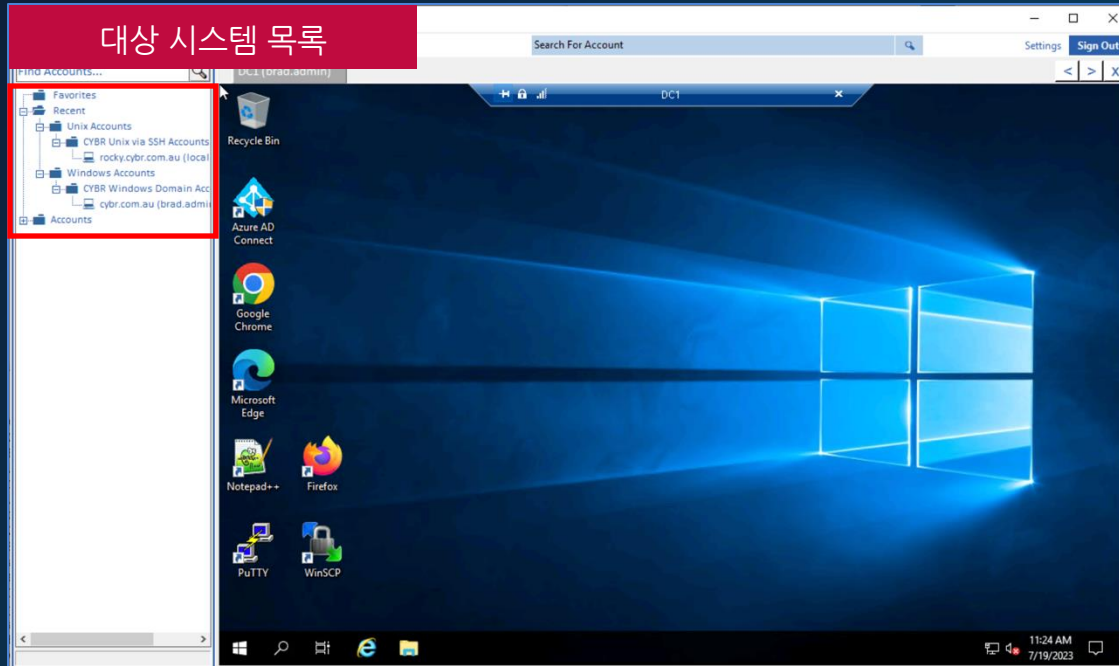
- **Isolates** 기업내 중요 서버 접속에 대한 세션 분리 제공
- **Secure** 효율적인 접속 관리 및 보안을 위한 단일 포인트 제공
- **Audit** 대상 시스템 접속 세션 활동에 대한 감사 제공



CYBERARK 웹 포탈 - OR - 선호 방식의 어플리케이션

주요 기능# 대상 시스템 접속 프로그램

단일화된 Client 프로그램 또는 웹 포탈을 통해 대상 시스템에 권한 접속 지원



주요 기능# 데이터베이스 권한관리

SQL패스워드 관리 및 철회제어, NoSQL 권한관리 지원

The screenshot displays the CyberArk Privileged Cloud Monitoring interface. The left sidebar contains navigation options: Privilege Cloud, System Health, Accounts, Accounts Feed, Accounts & Requests, PSM For SSH MFA Caching, Privileged Sessions, Monitoring (selected), Monitoring (Classic UI), Policies, Applications, Reports, and Help. The main panel is titled 'Monitoring' and shows a list of recordings. A red box highlights the 'Database Query Log' (데이터베이스 쿼리기록) section. The right panel shows the details of a session for 'tamir.benari@cyberarklab.com', including a 'Play' button and a list of activities. A red box highlights the 'Session Recording Play' (세션 레코딩 플레이) button. The activities list shows SQL commands executed on August 01, including a SELECT statement, a BEGIN statement, and two more SELECT statements.

Monitoring

Filter

Recordings Active sessions

39 results for: Sessions a... [Clear all filters](#)

Risk	Session	Play
-	j...	Play
-	j...	Play
-	c...	Play
60	j...	Play
-	j...	Play
-	j...	Play
-	a...	Play
-	t...	Play
-	t...	Play
-	t...	Play
-	t...	Play
-	t...	Play

세션 레코딩 플레이 **Play**

데이터베이스 쿼리기록

tamir.benari@cyberarklab.com connected as | [Additional details & actions in classic interface](#)

Start: 8/1/2023 03:42 PM Duration: 00:41:52

Activities Details

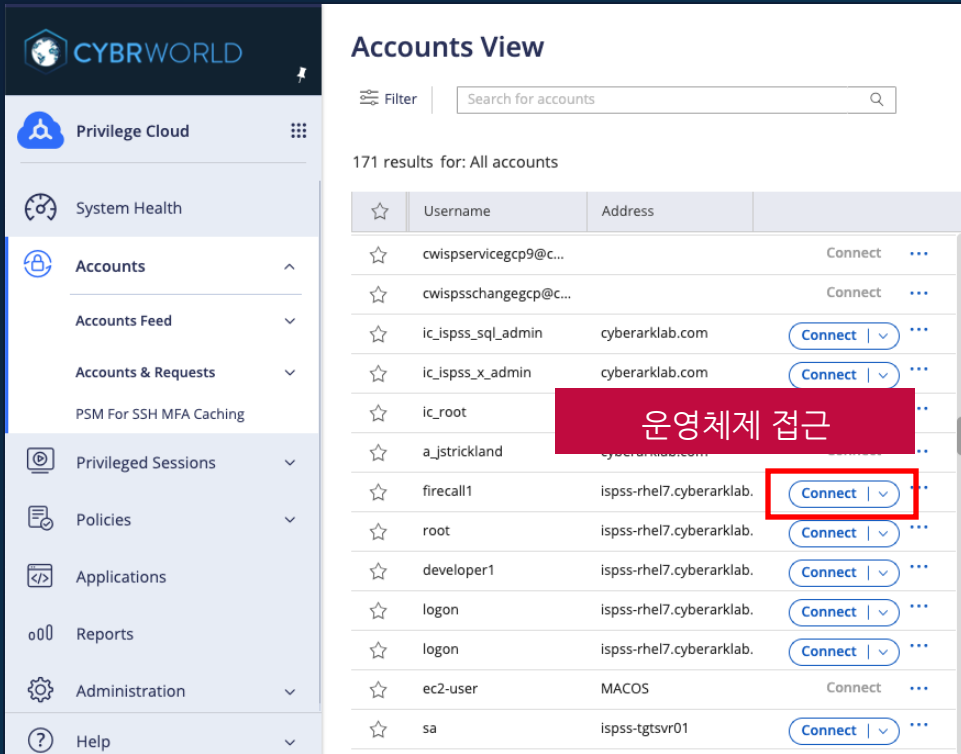
6 Activities in the session

Aug 01 Tuesday

- 3:42:35 PM SQLCommand | SELECT DECODE(USER, 'XS\$NULL', XS_SYS_CONTEXT('XS\$SESSION','USERNAME'), USER) FROM SYS.DUAL
- 3:42:35 PM SQLCommand | BEGIN DBMS_APPLICATION_INFO.SET_MODULE(1,NULL); END;
- 3:42:54 PM SQLCommand | select * from dual
- 3:43:02 PM SQLCommand | select sysdate from dual

주요 기능# 운영체제

단일화된 Client 프로그램 또는 웹 포탈을 통해 대상 시스템에 권한 접속 지원

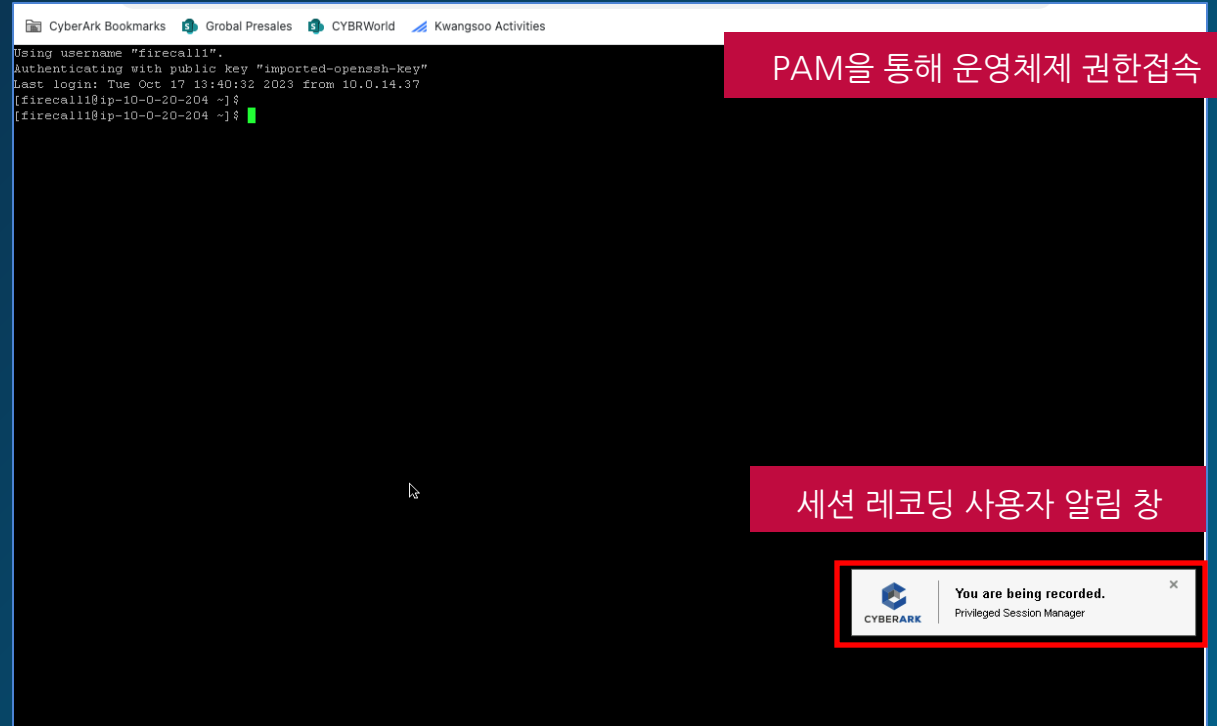


Accounts View

Filter | Search for accounts

171 results for: All accounts

☆	Username	Address	
☆	cwispservicegcp9@c...		Connect ...
☆	cwispschangegecp@c...		Connect ...
☆	ic_isps_sql_admin	cyberarklab.com	Connect ...
☆	ic_isps_x_admin	cyberarklab.com	Connect ...
☆	ic_root		...
☆	a_jstrickland		...
☆	firecall1	ispss-rhel7.cyberarklab.	Connect ...
☆	root	ispss-rhel7.cyberarklab.	Connect ...
☆	developer1	ispss-rhel7.cyberarklab.	Connect ...
☆	logon	ispss-rhel7.cyberarklab.	Connect ...
☆	logon	ispss-rhel7.cyberarklab.	Connect ...
☆	ec2-user	MACOS	Connect ...
☆	sa	ispss-tgtsvr01	Connect ...



CyberArk Bookmarks | Grobal Presales | CYBRWorld | Kwangsoo Activities

```
Using username "firecall1".
Authenticating with public key "imported-openssh-key"
Last login: Tue Oct 17 13:40:32 2023 from 10.0.14.37
[firecall1@ip-10-0-20-204 ~]$
[firecall1@ip-10-0-20-204 ~]$
```

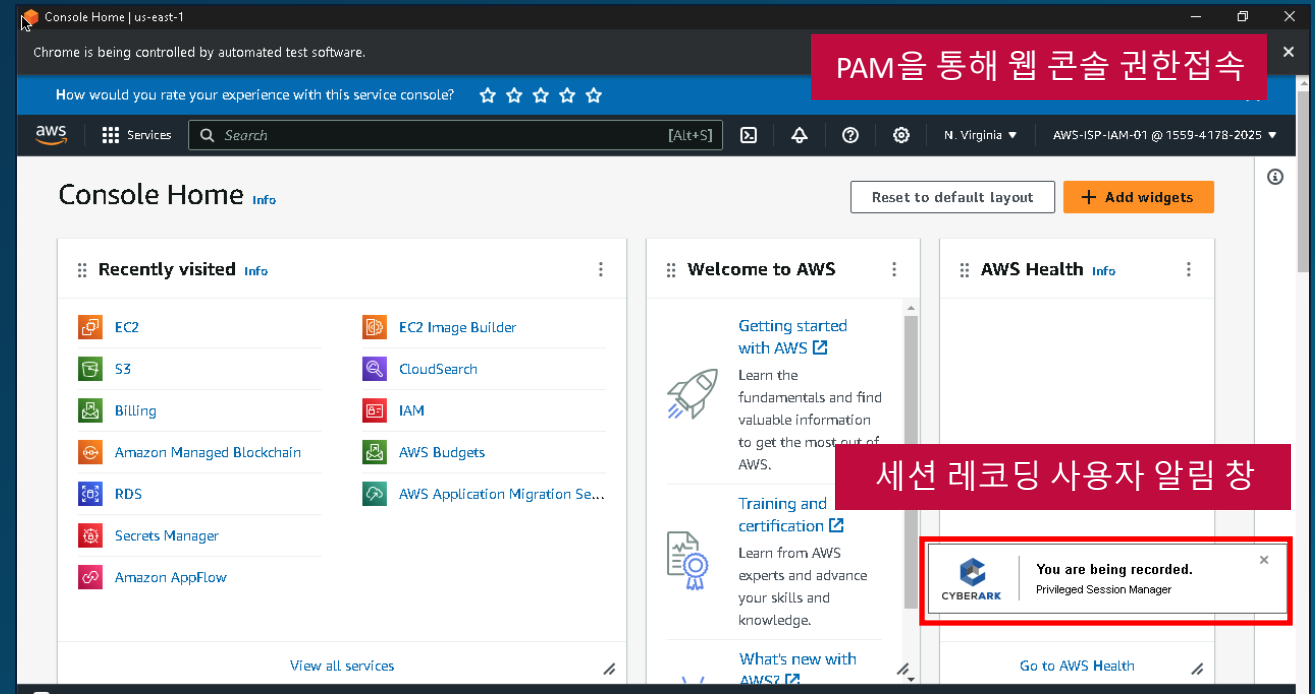
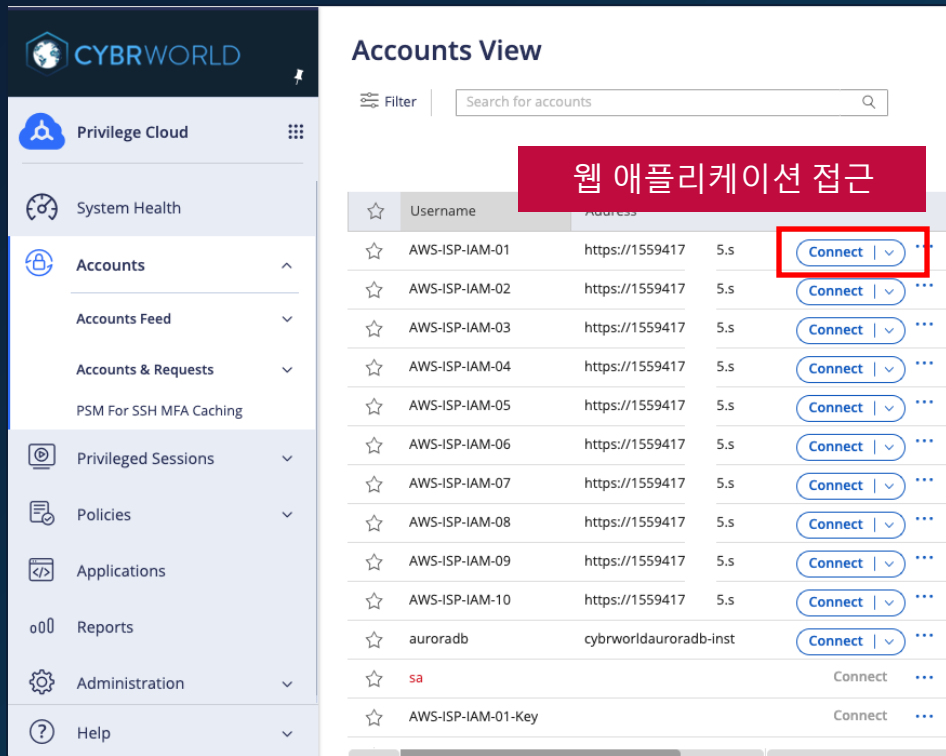
PAM을 통해 운영체제 권한접속

세션 레코딩 사용자 알림 창

You are being recorded.
Privileged Session Manager

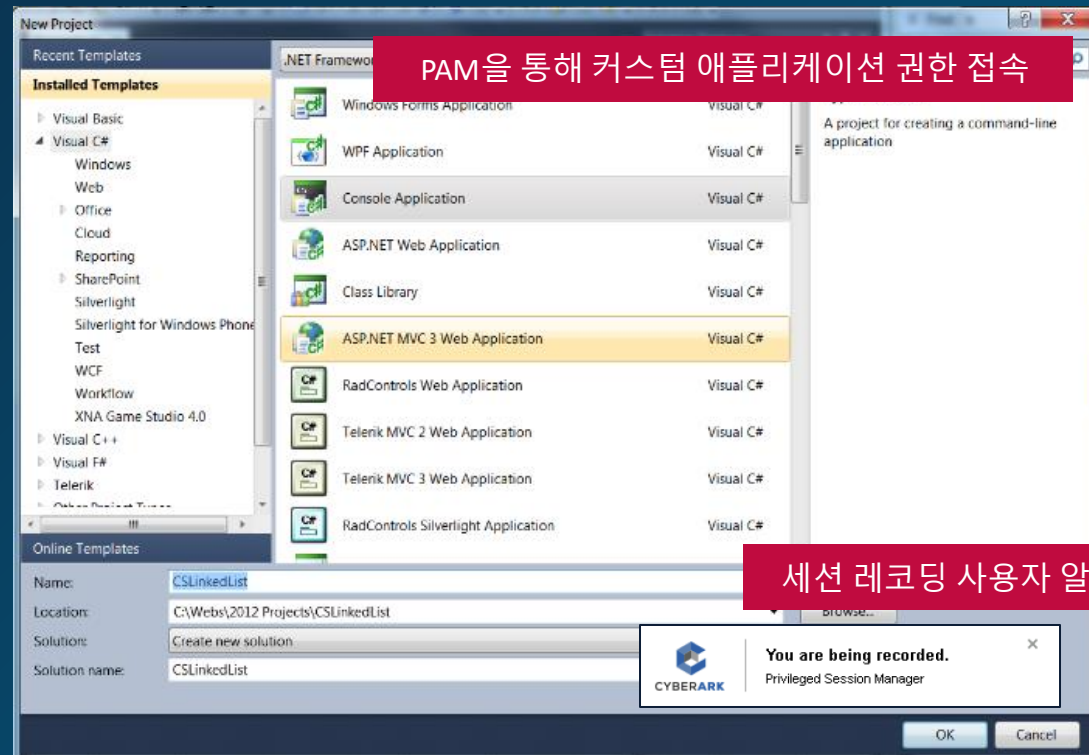
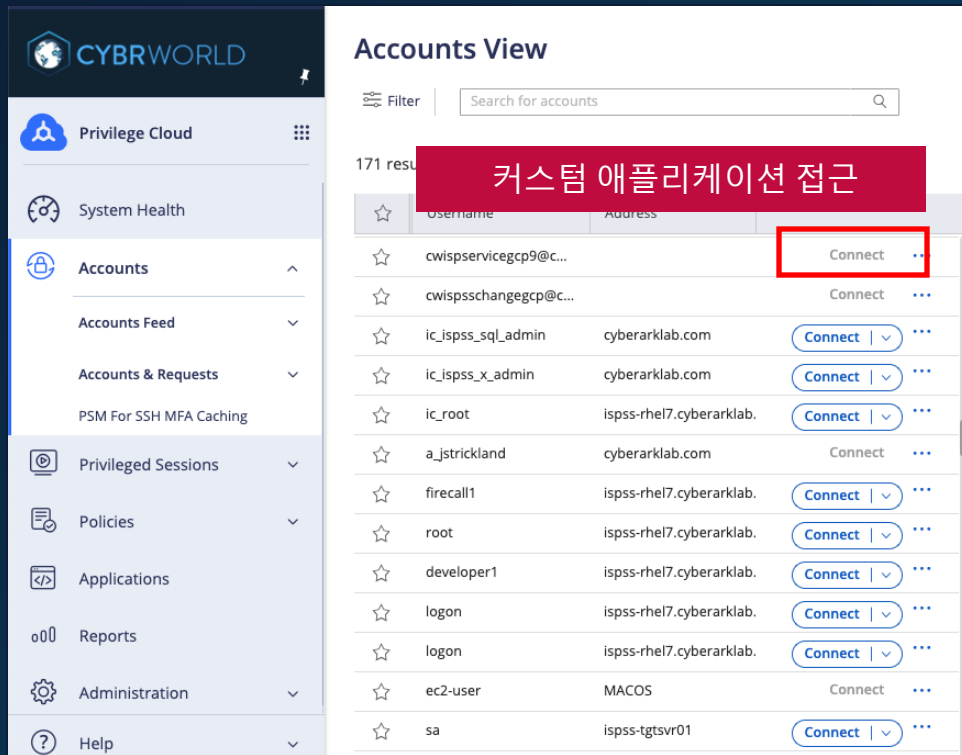
주요 기능# 웹 애플리케이션 권한관리

그룹웨어, CSP콘솔, 보안솔루션 등 모든 웹 애플리케이션 권한관리 지원



주요 기능# 커스텀 애플리케이션 권한 관리

직접 개발한 커스텀 애플리케이션 권한관리 지원



주요 기능# 네트워크 장치 권한관리

SSH프로토콜을 통해 접근하는 모든 네트워크 장치 권한 관리 및 비밀번호 관리


CYBRWORLD


Privilege Cloud


System Health


Accounts


Accounts Feed


Accounts & Requests


PSM For SSH MFA Caching


Privileged Sessions


Policies


Applications


Reports


Administration


Help

Accounts View


Filter

171 results for: All accounts

★	Name	Domain	Action
★	i_admin	CYBERARKLAB.COM	Connect ▼
★	adminy-admin	cybr.com	Connect ▼
★	xsa	cybr.com	Connect ▼
★	isp_t_admin	CYBERARKLAB.COM	Connect ▼
★	isp_t_admin1	CYBERARKLAB.COM	Connect ▼
★	isp_t_admin10	CYBERARKLAB.COM	Connect ▼
★	isp_t_admin2	CYBERARKLAB.COM	Connect ▼
★	isp_t_admin3	CYBERARKLAB.COM	Connect ▼
★	isp_t_admin4	CYBERARKLAB.COM	Connect ▼
★	isp_t_admin5	CYBERARKLAB.COM	Connect ▼
★	isp_t_admin6	CYBERARKLAB.COM	Connect ▼
★	isp_t_admin7	CYBERARKLAB.COM	Connect ▼
★	isp_t_admin8	CYBERARKLAB.COM	Connect ▼

```
COM3 PuTTY
LABSWITCH>
LABSWITCH>
LABSWITCH>
LABSWITCH>
LABSWITCH>
LABSWITCH>
LABSWITCH>
LABSWITCH>
LABSWITCH>
LABSWITCH>
LABSWITCH>
LABSWITCH>
LABSWITCH>
LABSWITCH>
LABSWITCH>
LABSWITCH>
LABSWITCH>enable
LABSWITCH#write e
LABSWITCH#write erase
Erasing the nvram filesystem will remove all configuration files!
Proceed with erase? [confirm] y[OK]
Erase of nvram: complete
LABSWITCH#
*Mar  1 00:05:57.405: %SYS-7-NV_BLOCK_INIT: Init of NV configuration block complete
LABSWITCH#reload
Proceed with reload? [confirm]
```

글로벌 기술 파트너# C3 Alliance

230+ Certified Partners



360+ Certified Joint Solutions

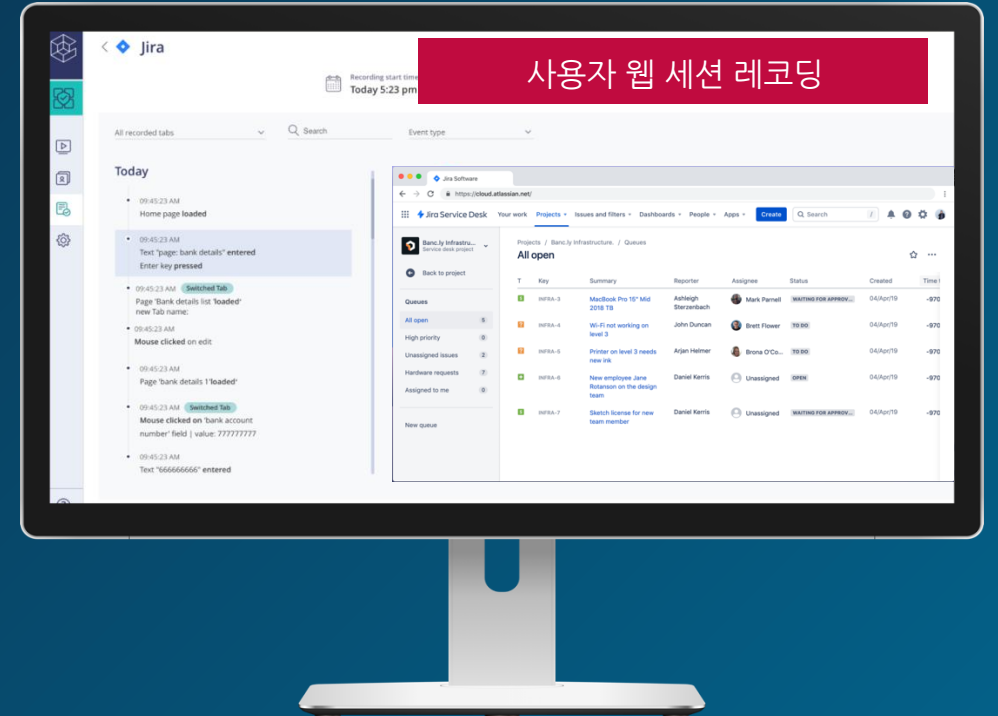
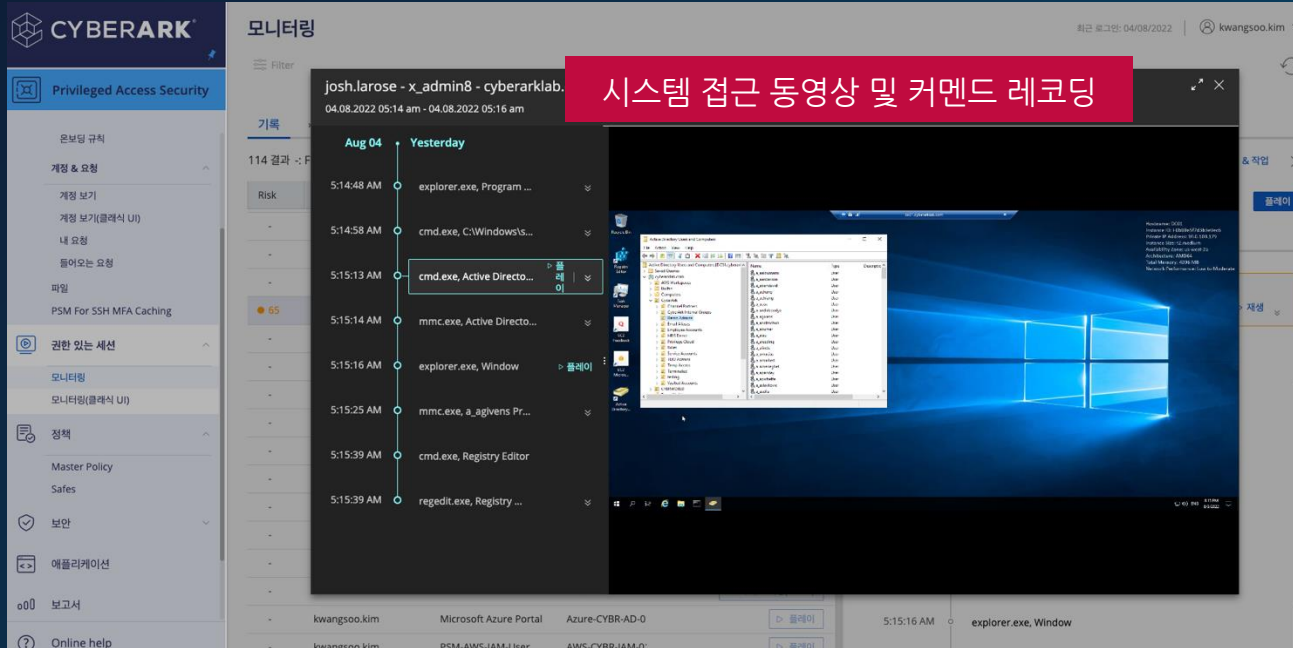


200+ Plug-ins



주요 기능# 세션 레코딩

시스템 작업 내역 및 사용자 웹 세션 모든 행위 레코딩



주요 기능# 위험 세션 탐지 및 대응

모든 접속 세션의 행위 분석을 통한 위협 탐지 및 대응 (세션 중지, 종료 및 모니터링)



주요 기능# 위험 세션 탐지 및 대응

위험 탐지에 따른 위험점수 기반의 이벤트 제공

Privileged Access Security

온보딩 규칙

계정 & 요청

계정 보기

계정 보기(클래식 UI)

내 요청

들어오는 요청

파일

PSM For SSH MFA Caching

권한 있는 세션

모니터링

모니터링(클래식 UI)

정책

Master Policy

Safes

보안 사건

Filter

5 의심스러운 세션 활동 탐지

Aug 04 Yesterday

9:41:33 PM
100 HIGH

권한 있는 세션에서 의심스러운 활동이 감지됨 수정 시작됨

권한 있는 세션에서 <https://portal.azure.com>의 의심스러운 세션 활동이 감지되었습니다.

이 세션은 Azure-CYBR-AD-01@cyberark365globalabs.onmicrosoft.com@<https://portal.azure.com> 계정을 가진 Vault 사용자 amit.bendavid이(가) Task Manager - Google Chrome 활동을 실행하여 시작되었습니다.

ID 62ebbe7fe4b0c59a465aa63b

Close

세션 ID 0fca164e-f49a-4750-b8f4-f52a003e9b95

권장

세션 종료 요청이 시작되었습니다. 세션 및 해당 활동과 관련된 각 보안 이벤트를 검토하고 추가 대응이 필요한지 평가하십시오.

8:42:51 PM
MEDIUM

비관리 권한 계정 수정 시작됨

계정 stefen.jwZwRFwn4fxk8@tgtsvr01.cyberarklab.com이(가) tgtsvr01.cyberarklab.com에서 로컬 권한 그룹 Administrators에 추가되었지만 이 계정은 CyberArk PAS에서 관리되지 않습니다.

ID 62ebb0d2e4b0c59a465a26ce

Close

주요 기능# 위험 세션 탐지 및 대응

특정 명령어 수행에 따라 위험 점수 및 행위 발생에 따른 대응(차단, 중지, 모니터링) 설정

보안 구성

자격 증명 조정

권한 있는 세션 분석 및 대응

위험요소별 점수 및 대응 설정

카테고리	패턴	점수	설명	응답	상태
SSH	(.*)id_rsa.pub(.*)	50	Indication of access to Linux key stores might be indica...	없음	활성 상태
SSH	(.*)identity.pub(.*)	50	Indication of access to Linux key stores might be indica...	없음	활성 상태
SSH	(.*)useradd(.*)	60	Indication of adding a user, which could indicate the cre...	일시 중지	활성 상태
SSH	(.*)history(.*)	70	represents a set of commands that may indicate a use...	일시 중지	활성 상태
SSH	(.*)authorized_keys(.*)	60	Manipulation of SSH keys on the machine. Could indica...	없음	활성 상태

보안 구성

자동 수정

계정 자동 은보드

자격 증명 순환

자격 증명 조정

- 관리되지 않는 계정 등록
- 패스워드 강제 변경
- 세션 강제 종료 또는 중지

정규식 패턴 지원

규칙 편집

패턴

세션 응답

점수

root01@unx1:~

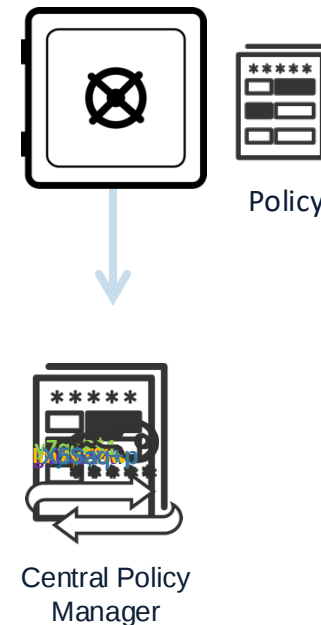
root01@unx1 ~]\$ passwd

YOUR SESSION HAS BEEN SUSPENDED

주요 기능# 패스워드 및 SSH Key관리

특정 명령어 수행에 따라 위험 점수 및 행위 발생에 따른 대응(차단, 중지, 모니터링) 설정

사이버아크의 솔루션에서는 일반적인
패스워드는 물론 SSH key에 대한
변경관리까지 제공함



IT Environment

System	User	Pass
Unix	root	tops3cr3t
Oracle	SYS	tops3cr3t
Windows	Administrator	tops3cr3t
z/OS	DB2ADMIN	tops3cr3t
Cisco	enable	tops3cr3t

주요 기능# 안전한 원격접속 환경 제공

VPN-less 구성으로 비용절감 및 편리한 원격접속 환경 제공



VPN-less, Password-less



안전한 원격 접속
업무환경



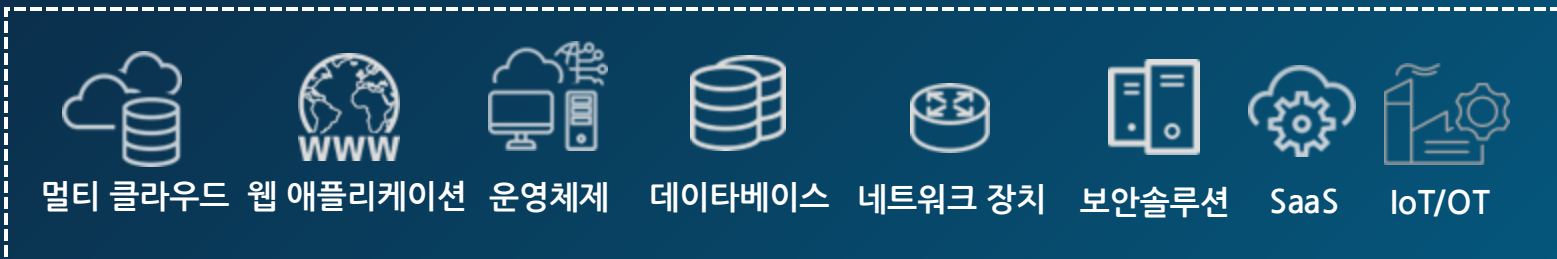
사이버아크
VPN-less 원격 접속
솔루션(Vendor PAM)



사이버아크
차세대 시스템접근제어



세션 이원화, 모니터링 및 제어
제공

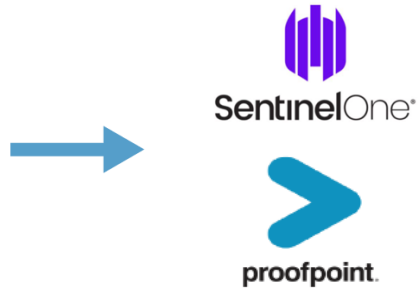


주요 기능# 다양한 보안 솔루션 연동

3rd 보안 솔루션 연동을 통해 감염된 단말을 통한 액세스 차단



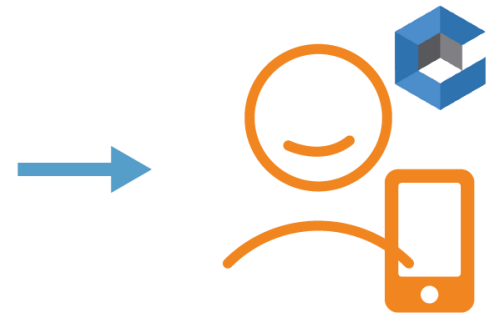
보안 솔루션을
통해 감염 단말
정보 수집



특정 임계치 초과 시



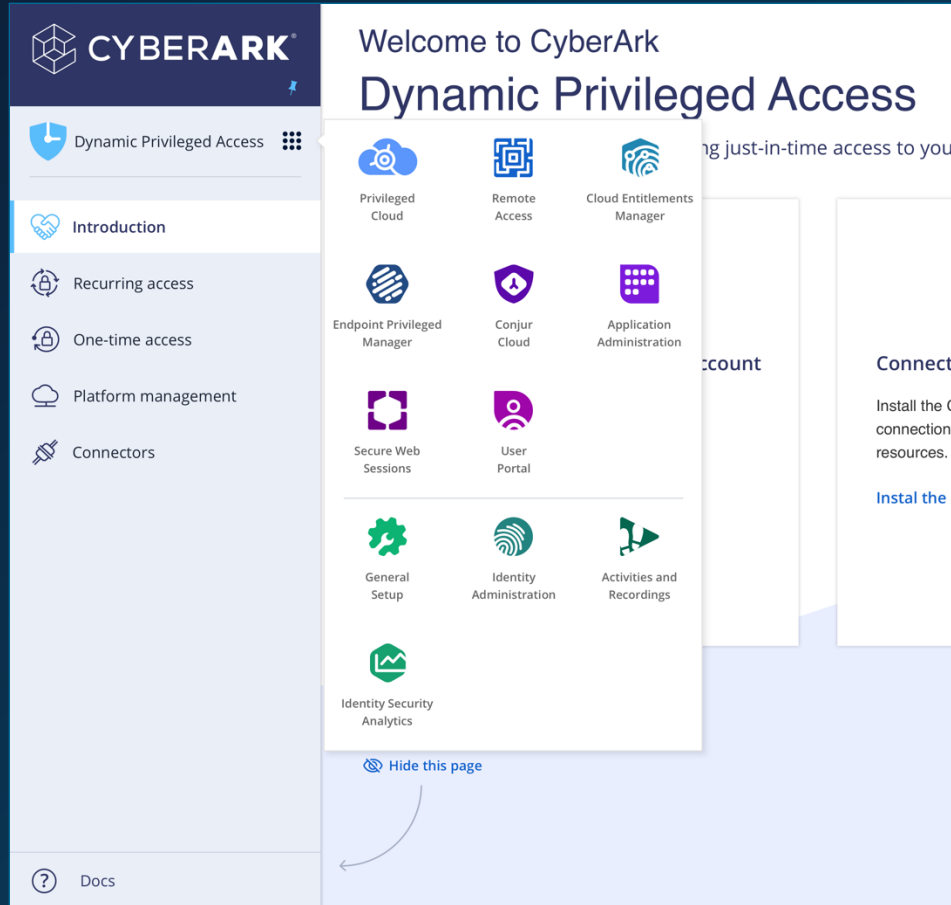
감염 의심 사용자
그룹으로 사용자 이동



의심 사용자 시스템
액세스 제한

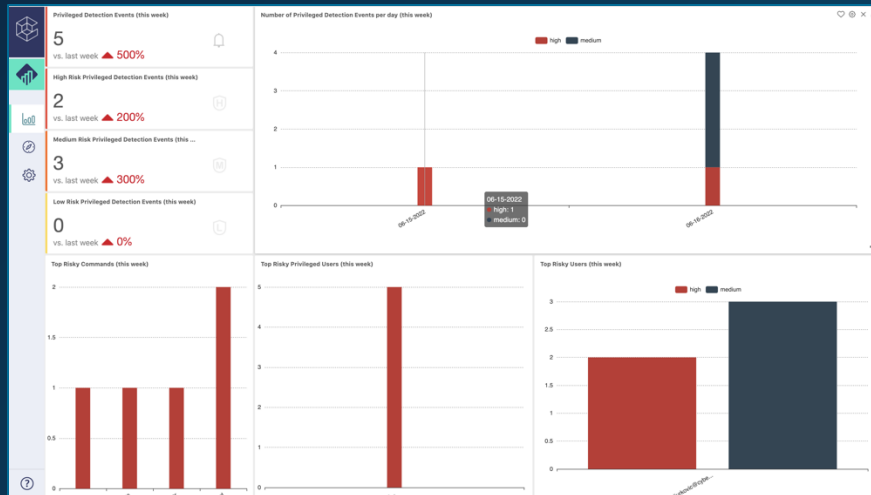
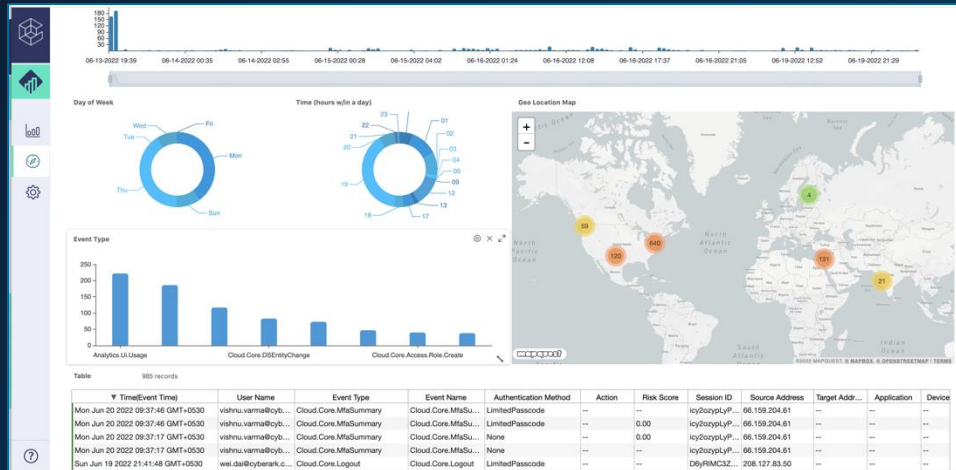
주요 기능# 통합 관리콘솔

SSO포탈을 통해 통합된 차세대 시스템접근제어 운영



주요 기능# 통합 아이덴티티 위협 분석

사용자 이상 행위 및 잘못된 권한 계정 사용에 대한 탐지, 조사 및 대응 제공



이상 행위 및 위협에 대한 탐지 및 예방을 위한 통합 플랫폼:

- SSO/MFA를 통한 웹 접속 제공
- 권한 계정 현황 제공

주요 특징:

- 사용자 행위 및 통합적인 위협 확인을 위한 통합 인사이트 UI 제공
- SIEM 시스템 등으로의 보안 이벤트 전달
- 감사, 컴플라이언스 및 포렌식 등의 신속한 대응을 위한 위협 점수 제공
- 자동화 및 권장 대응 제공

업무 브라우저 분리

업무용 브라우저

- 자격 증명 정보
- 데이터



사이버아크 시큐어 브라우저

개인용 브라우저

- 자격 증명 정보
- 데이터





웹 애플리케이션

Search Google or type a URL

운영체제, 네트워크, 데이터베이스 등 시스템 자원

- Noun Project
- תרגום מורפיקס
- WhatsApp
- Dribbble
- Shutterstock
- (224) Pinterest
- Spotify
- User Portal
- Facebook
- Add shortcut

업무 이벤트

Secure Browser

Applications

AWS

Azure

GCP

Kubernetes

Docker

Lacework

See more

Privilege Cloud - Targets

Helpdesk_ad6578078@ma.com
https://cyberark smartfile.com/

Helpdesk_ad6578078@ma.com
https://cyberark smartfile.com/

Helpdesk_ad6578078@ma.com
https://cyberark smartfile.com/

See more

Jira tasks

DIGI-6488
Error 500 on pcloud-pvwa-um-...

DIGI-6488
Error 500 on pcloud-pvwa-um-...

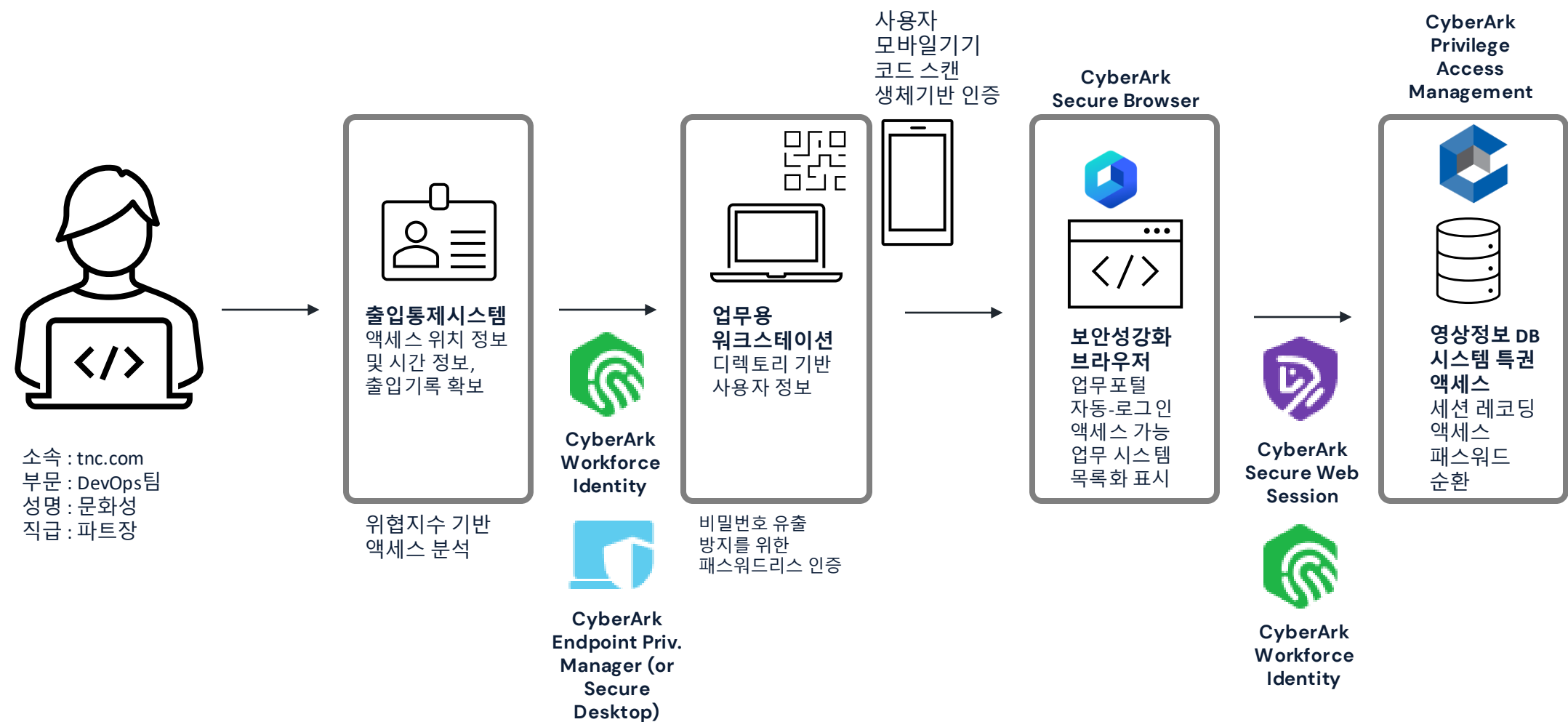
DIGI-6488
Error 500 on pcloud-pvwa-um-...

DIGI-6488
Error 500 on pcloud-pvwa-um-...

DIGI-6488
Error 500 on pcloud-pvwa-um-...

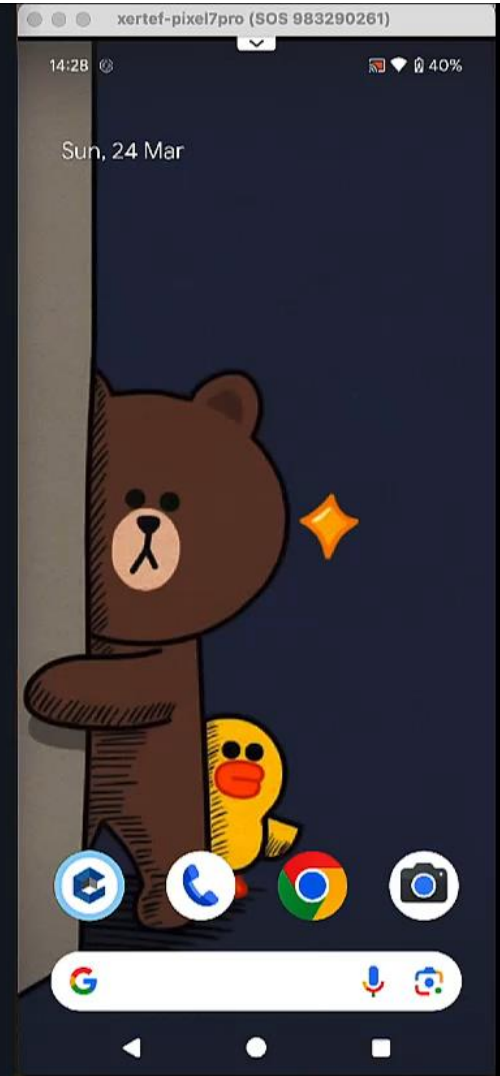
See more

Password-less 시나리오



Demo

2:28
Sunday, March 24



Summary



가장 완전한 차세대 시스템접근제어 PAM

제로 트러스트 아키텍처 기반의 멀티 클라우드&하이브리드 환경의 차세대 시스템접근제어 제공



가장 현대적인 아이덴티티 솔루션

SSO, MFA, 계정 라이프사이클 관리, 디렉토리 서비스, 운영체제, 데이터베이스, 애플리케이션 등등 최상의 차세대 시스템접근제어 기능 제공



포괄적인 시스템 연동

가장 많은 3rd 상용 애플리케이션, In-House 애플리케이션 연동을 통해 차세대 아이덴티티 신원 보안 제공



아이덴티티 보안의 리더

가장 복잡한 IT보안, 특권 계정 관리, 액세스 관리를 성공적으로 수행하기 위해 기술을 개발하고, 새로운 위협에 대응하는 도전정신으로 시장 선도



다양한 환경의 아이덴티티 보안 경험

글로벌 Top 기업 및 조직에서의 폭넓은 아이덴티티 신원 보안 구성 경험을 통해 최적의 솔루션 제공



CYBERARK[®]
The Identity Security Company[™]

Thank You

<https://www.cyberark.com>

제로 트러스트 가이드라인 1.0

과학기술정보통신부가 새로운 디지털 환경 정보보안 추진을 위해 지난 6월 '제로트러스트 가이드라인 1.0' 발표



CONTENTS	
I. 제로트러스트 추진배경	8
■ 환경의 변화	8
■ 기존 경계 기반 보안모델의 한계	9
■ 미국의 제로트러스트 동향	10
■ 참고 1 최근 국내외 침해사고 분석	11
II. 제로트러스트 소개	12
■ 제로트러스트 개념	13
■ 제로트러스트 보안원리	14
■ 참고 2 기존 경계 기반 VS 제로트러스트 보안모델 비교	15
III. 제로트러스트 아키텍처	16
■ 제로트러스트 기본철학 및 핵심원칙	17
■ 제로트러스트 접근제어 원리	18
■ 참고 3 글로벌 기업의 사례	20
IV. 제로트러스트 도입	22
■ 제로트러스트 도입 계획	23
■ 제로트러스트 도입을 위한 기업망 핵심요소	24
■ 제로트러스트 성숙도 모델	25
■ 제로트러스트 도입 전후 비교	26
V. 제로트러스트 도입 참조모델	27
■ COVID-19 이전 원격근무 환경	28
■ COVID-19 이후 일반화된 원격근무 환경	29
■ 일반적 원격근무 환경에 대한 공격 사례	30
■ 안전한 원격근무를 위한 제로트러스트 참조 모델	33
VI. 참고문헌	36

가이드라인에서 명시한 제로
트러스트 구현 핵심 원칙에 따라
기업이 성공적으로 제로 트러스트
아키텍처를 도입할 수 있도록
솔루션 제공

제로 트러스트 가이드라인 1.0

제로 트러스트 구현 핵심원칙# 가이드 15페이지

사이버아크 차세대 아이덴티티 플랫폼

로그인 시간, 계정, 도메인, 접속 위치, 보안 상태 등 환경 적인 요소에 기반하여 차등 있는 인증 및 MFA 적용

게이트웨이 방식으로 대상시스템(자원)에 접근하는 모든 세션을 단일지점에서 관리하여 지속적인 신뢰 검증 및 레코딩

모든 대상 시스템 접근 로깅 및 레코딩 처리

〈제로트러스트 구현 핵심원칙〉

핵심 원칙	세부 내용
인증 체계 강화 (기본철학 중 ①②③⑥)	▲ 각종 리소스 접근 주체에 대한 신뢰도(사용하는 단말, 자산 상태, 환경 요소, 접근 위치 등을 판단)를 핵심요소로 설정하여 인증 정책 수립 ※ 기업내 사용자에 대한 여러 아이디를 허용하여 일관된 정책을 적용하지 않거나, 신뢰도 판단없이 단일 인증 방식만으로 접속을 허용할 경우 크리덴셜 스테핑에 취약
마이크로 세그멘테이션 (기본철학 중 ②④⑤)	▲ 보안 게이트웨이를 통해 보호되는 단독 네트워크 구역(segment)에 개별 자원(자원그룹)을 배치하고, 각종 접근 요청에 대한 지속적인 신뢰 검증 수행 ※ 개별 자원별 구역 설정이 없으면, 기업망 내부에 침투한 공격자가 중요 리소스로 이동하기 쉬워 공격이동 공격 성공 가능성이 높아짐
소프트웨어 정의 경계 (기본철학 중 ①②⑤)	▲ 소프트웨어 정의 경계 기법을 활용하여 정책 엔진 결정에 따르는 네트워크 동적 구성, 사용자 단말 신뢰 확보 후 자원 접근을 위한 데이터 채널 형성 ※ 클라우드 온프레미스로 구성된 기업 네트워크 내부에서 단말이 임의 데이터를 전송할 수 있다면, 네트워크 및 호스트 취약성에 따르는 피해 가능성이 커짐

[NIST SP 800-207, 제로트러스트 아키텍처에 대한 다양한 접근법(3.1절)을 기반으로 작성]