어플리케이션 접근통제를 통한 계정 침해 보호 및 AD 계정 침해 탐지전략

Solution Consultant / Hongso Chae

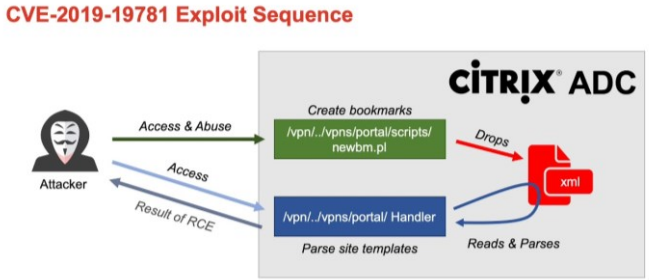
hongso.chae@quest.com

Quest

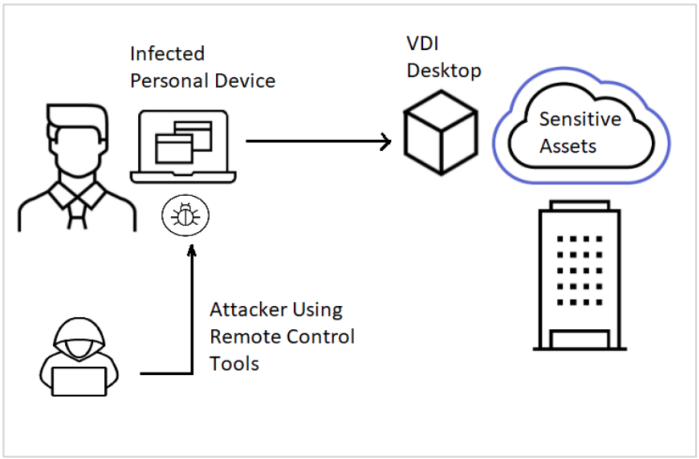
Where Next Meets Now.

VDI 기반 재택근무 환경의 보안 이슈

취약점을 이용하여 Citrix 서버 공격



개인단말 을 공격하여 내부로 접근



증가하는 보안 이슈

다크웹에 올라온 국내 기업 랜섬웨어 피해 사례 *해커들 주장

시기	기업	피해
2020년 5~8월	LG전자, SK하이닉스	내부 정보 유출
11월	이랜드 그룹	백화점 등 일부 매장 휴업
2021년 1분기	현대자동차 계열사	자동차 도면, 재무자료 등
4월	CJ셀렉타 브라질법인	직원 이메일 정보 등
	LG생활건강 베트남 법인	내부 문서 일부 유출
5월	LG전자 북미법인	제품 테스트 정보 등

개인·중소업체 랜섬웨어 피해 신고 (단위=건)

*2021년은 추정치. 한국랜섬웨어침해대응센터 신고만 집계한 것

많은 보안 위협이 단말에서 발생

(재택근무가 증가하면서 이러한 보안 이슈도 증가)

Quest

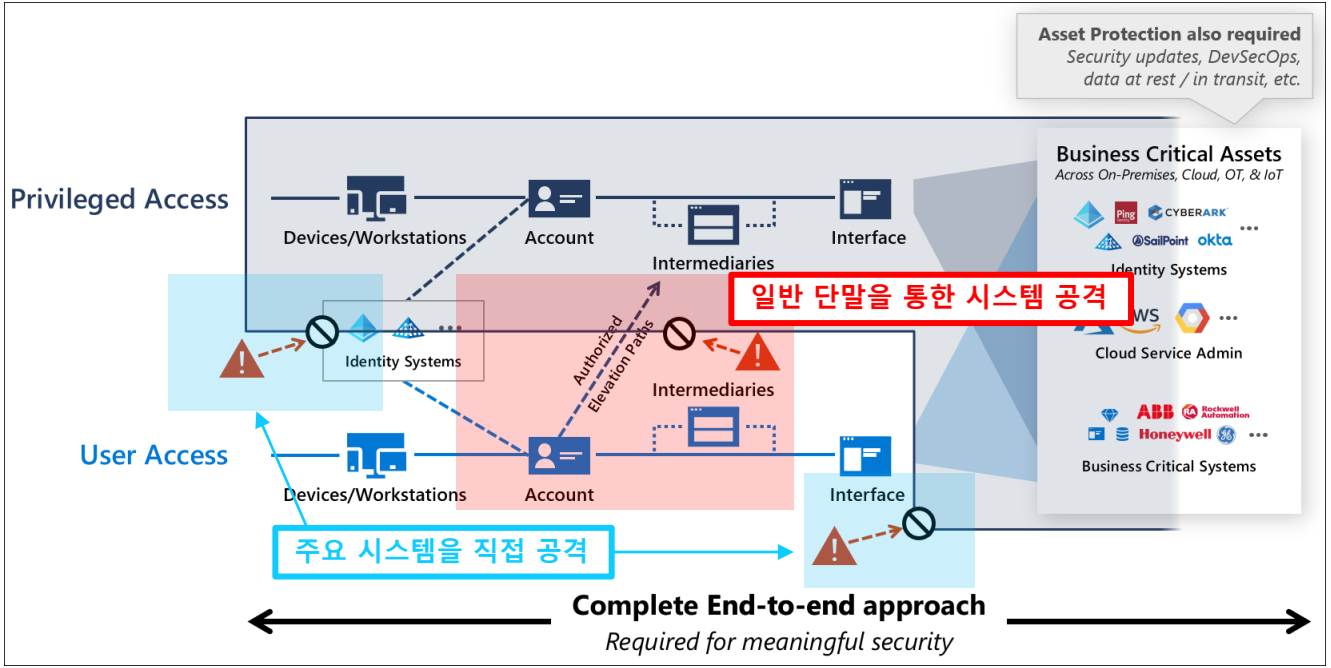
Where Next Meets Now.

이러한 환경의 변화와 증가하는

보안위협을 대응하기 위해서는

고도화된 내부 보안체계가 필요

주요 위협 접근 경로



공격의 핵심은 **계정**과 **권한**

일반 단말을 통한 시스템 공격

➡ Active Directory

주요시스템을 직접 공격

➡ 접근통제

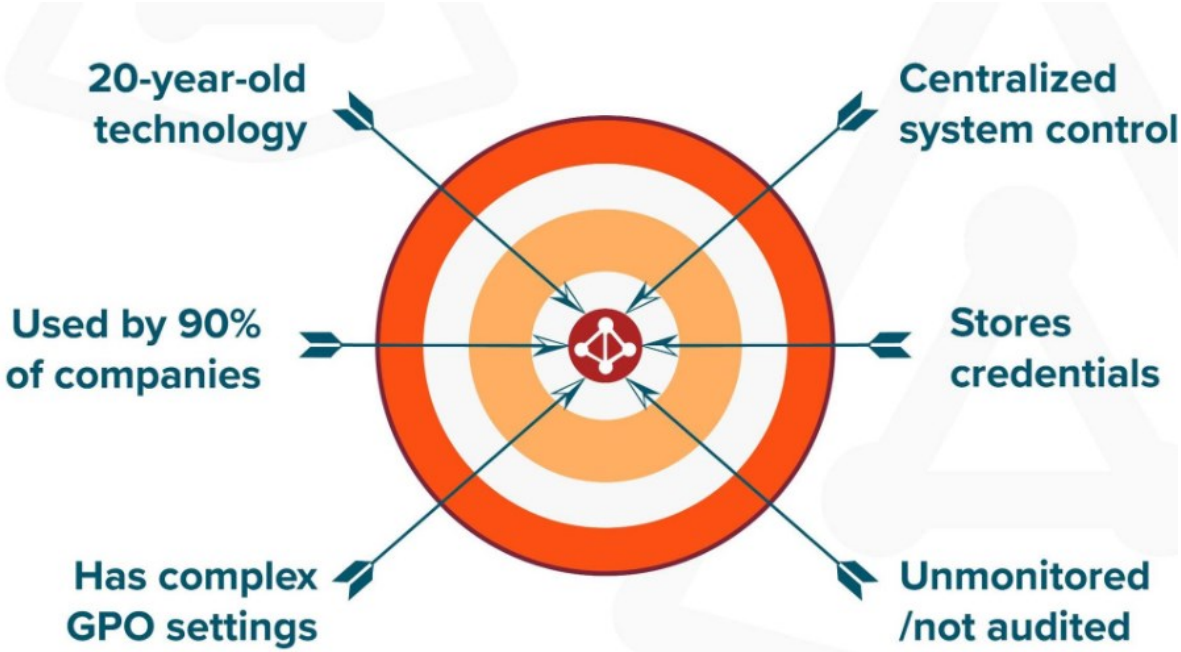
Privileged Access Strategy

Quest

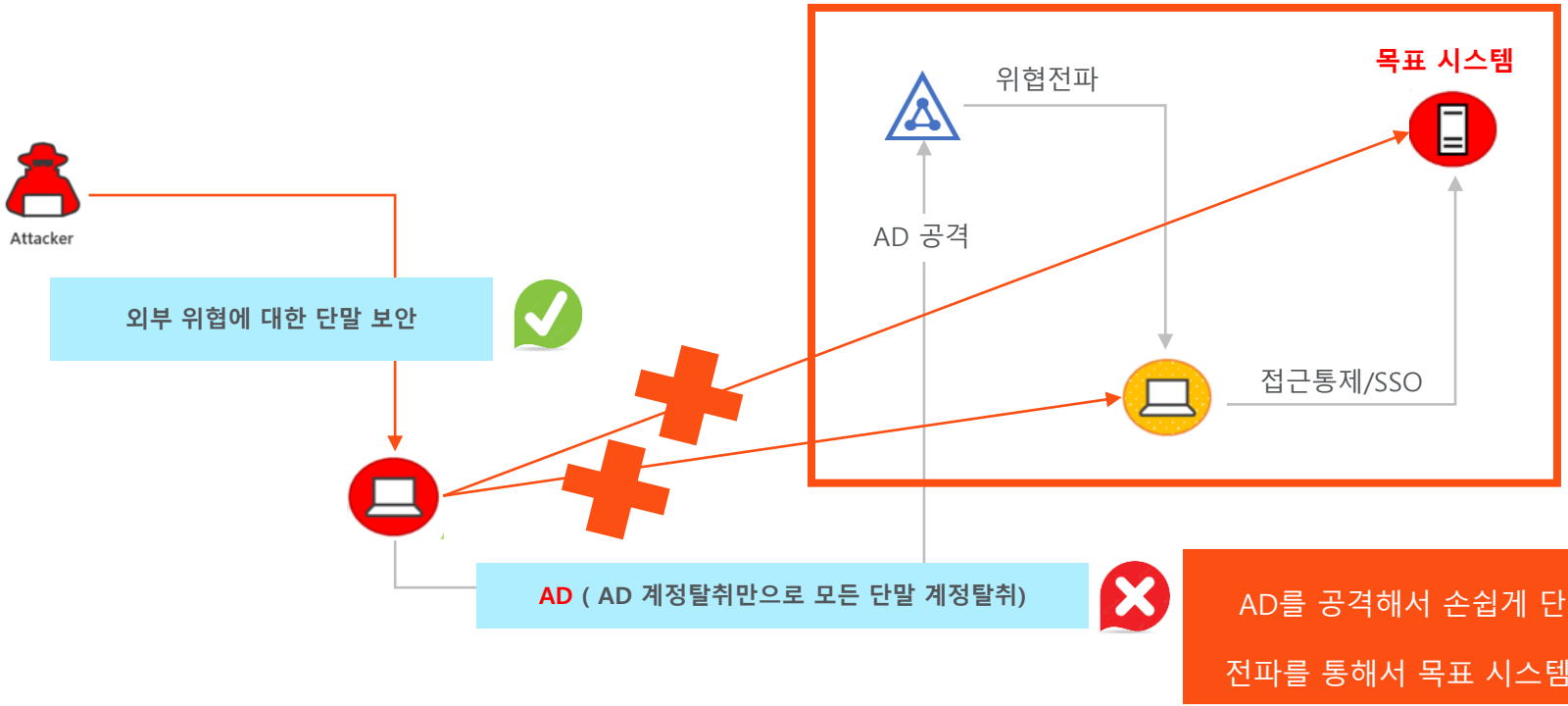
Where Next Meets Now.

Active Directory 보안이 되지 않으면?

AD는 Tier 0의 서비스로 주요한 공격 타겟



AD보안이 되지 않으면?


목표 시스템
위협전파
Attacker
AD 공격
외부 위협에 대한 단말 보안
접근통제/SSO
AD (AD 계정탈취만으로 모든 단말 계정탈취)
AD를 공격해서 손쉽게 단말간
전파를 통해서 목표 시스템 공격

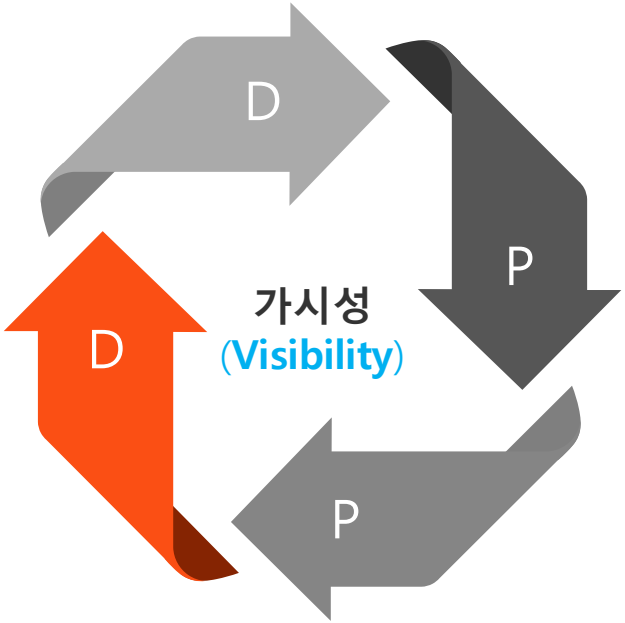
AD 보안전략(2P2D)

Diagnostic(분석)

운영과정에서의 분석 및 위협발생에 대한 원인분석을 위한 데이터 및 검색 체계

Prevent(예방)

위협이 될 수 있는 정책위반에 대한 탐지를 통해서 사전에 위협 탐지 및 대응



Detect(탐지)

AD에 알려진 위협 등을 통한 공격을 실시간으로 탐지하여 피해를 최소화

Protect(보호)

위협이 될 수 있는 요소를 보호하여 위협요소 사전 차단

AD 복구의 이슈 발생 사례

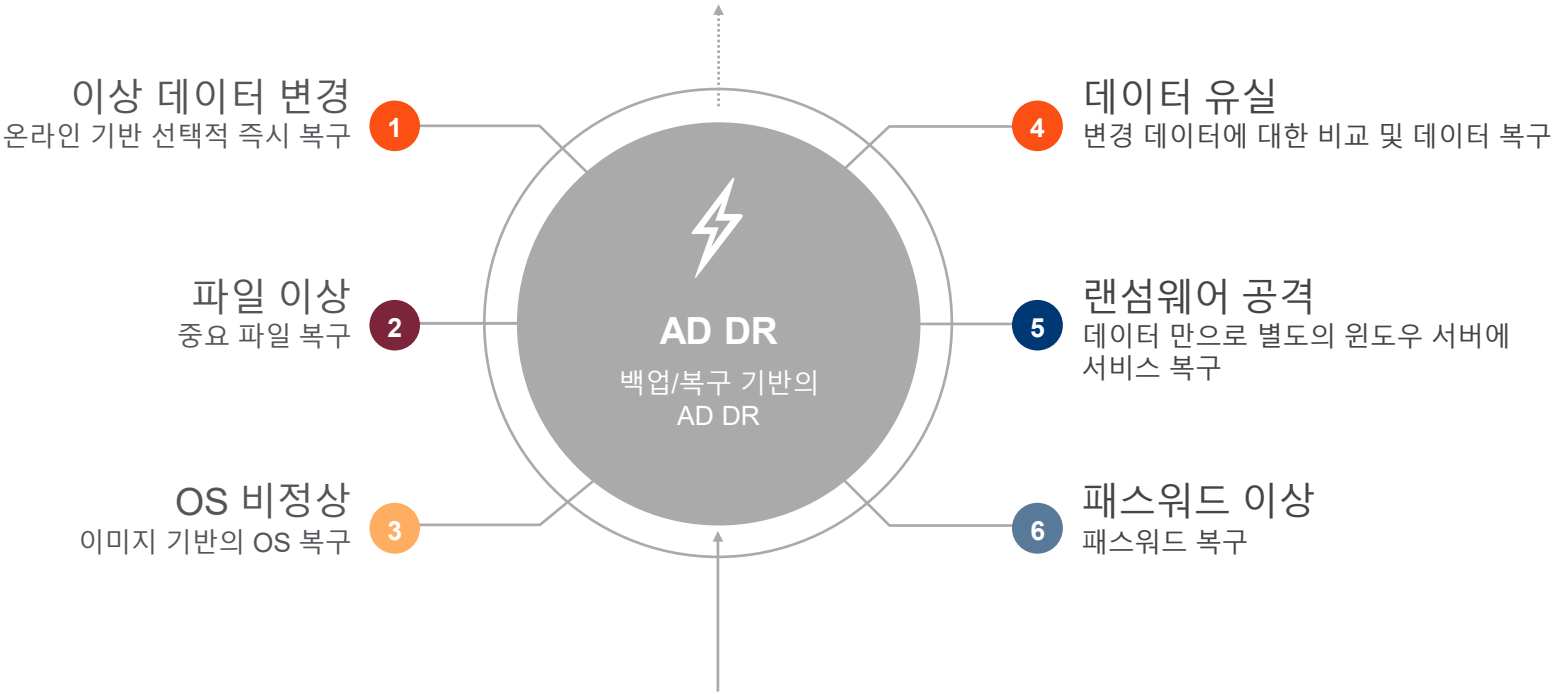
Maersk

- NotPetya로 150개 DC중 149개 유실
- AD복구에 9일이 걸림
- $$ Millions 손실
- 뉴스 해드라인 장식

국내 기업

- 랜섬웨어 공격
- 이전 OS 백업으로 복구
- Domain의 Trust가 깨져서 모든 단말에서 Domain 재 Join 수행
- Domain Join에 몇 주 소요

AD 전문 복구 기반의 DR 체계 필요사항



접근통제의 보안이 되지 않으면?

Quest

Where Next Meets Now.

privileged account는?

큰 피해를 줄 수 있는 힘을 가지고 있는 모든 가장 중요한 시스템의 계정

root

Administrator

Directories

amazon web services

Azure

Service Accounts

Built-in accounts

Network Devices

> **⚠ WARNING**
>
> **UNAUTHORIZED DATA ACCESS**
>
> - Secure access to the FTP/Web server using User Rights.
> - If you do not enable User Rights, disable the FTP/Web server to prevent any unwanted or unauthorized access to data in your application.
>
> **Failure to follow these instructions can result in death, serious injury, or equipment damage.**

MySQL

root

ORACLE

SYS / SYSTEM

Microsoft SQL Server

SQL

First ransomware-related death reported in Germany Sept 2020

Automation IoT

Critical Infrastructure

PLC

Coca-Cola

Social Media

SAP

by Quest

관리의 범위?

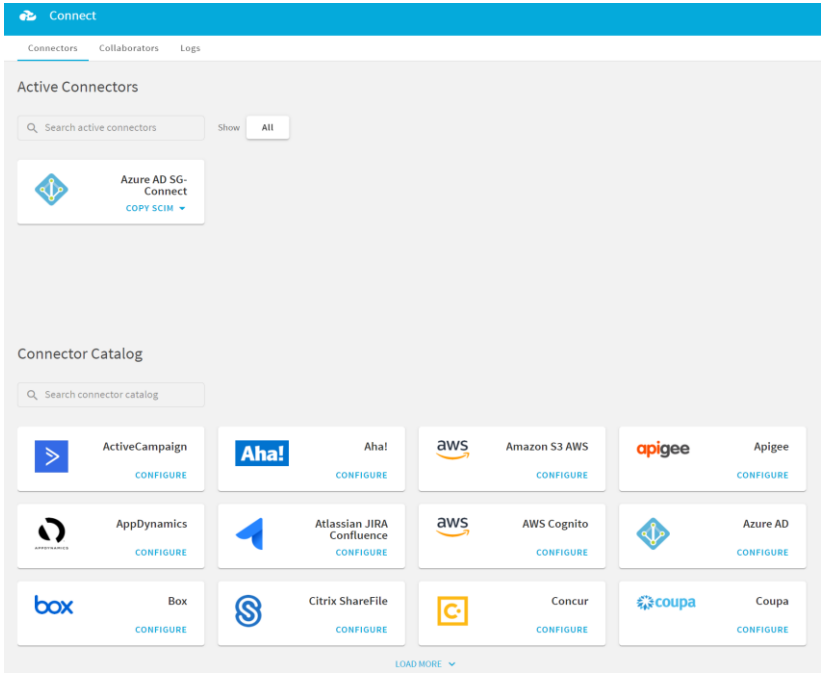
높은 권한으로 인하여 발생하는
보안/서비스 장애를 어디까지 관리할지 ?

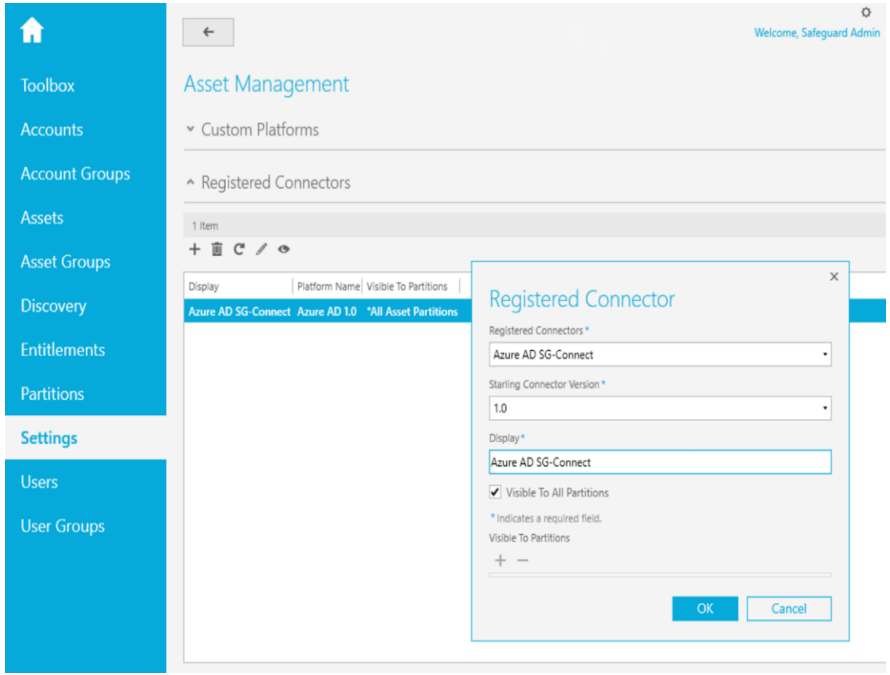
특권계정 사용자

Quest

Where Next Meets Now.

SaaS기반의 솔루션 (Azure, AWS Cloud 포함)

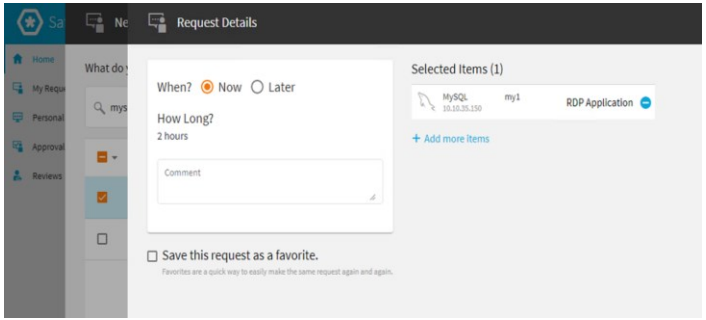


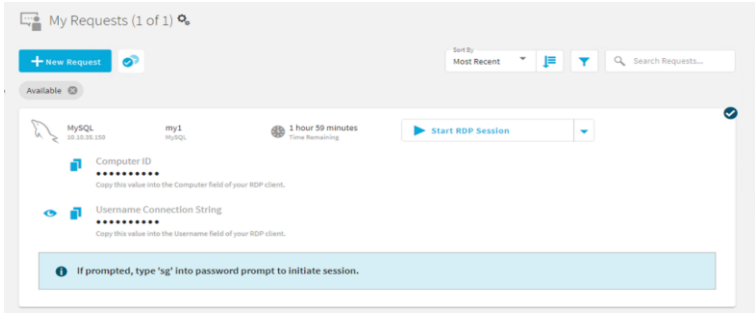


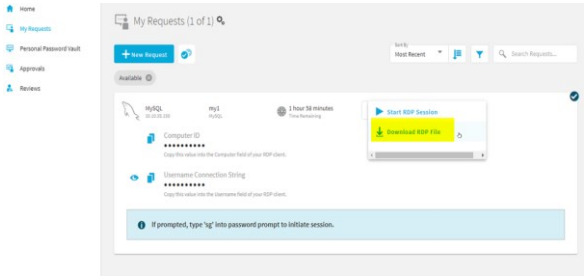
Quest

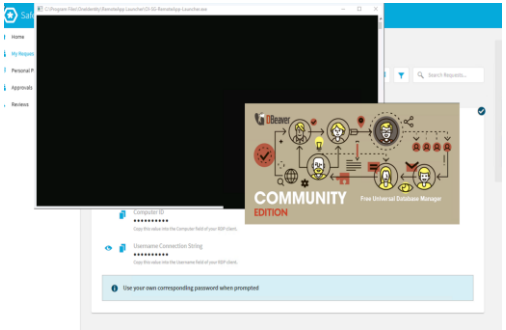
Where Next Meets Now.

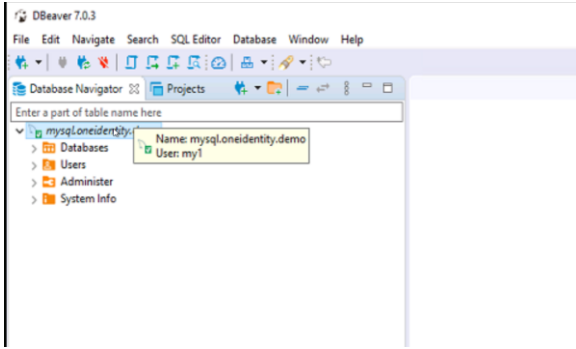
어플리케이션(웹, C/S) 접근통제











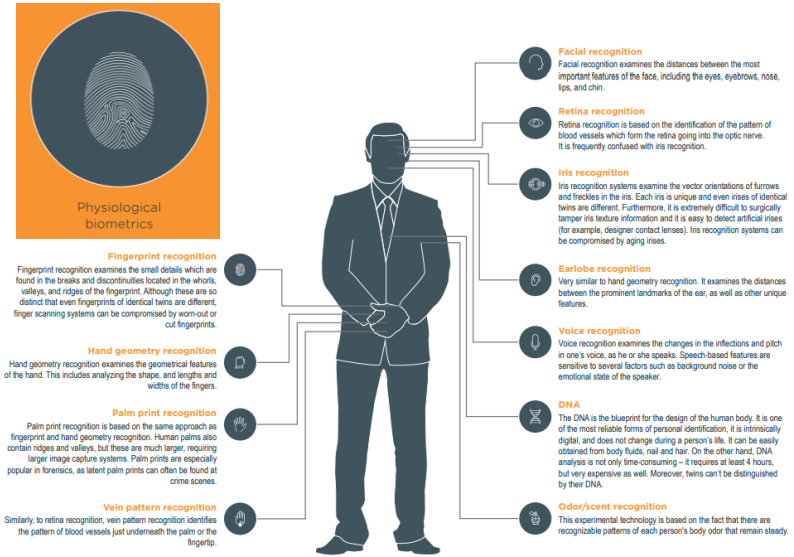
어플리케이션 접근통제 및

행위기반 위협분석 및 녹화

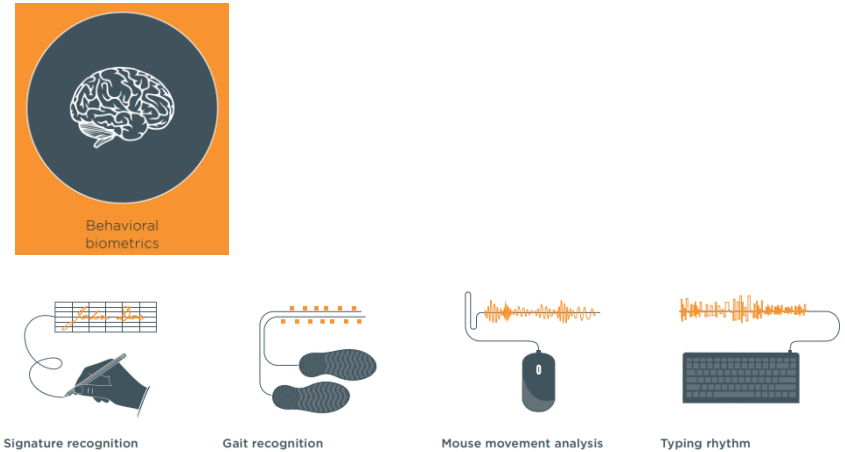
Quest

Where Next Meets Now.

2가지 형태의 생체정보

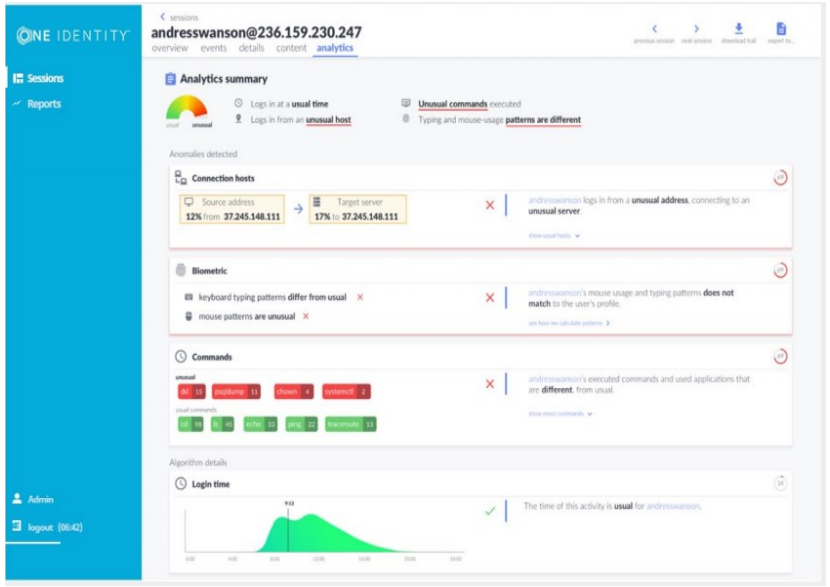


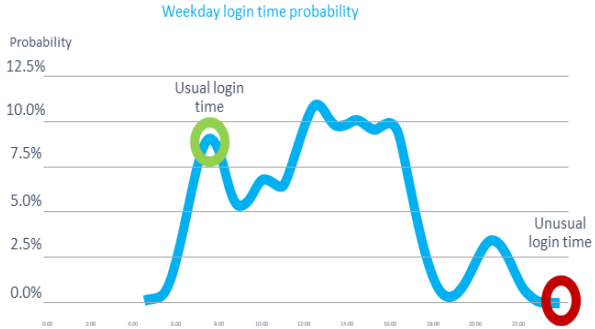
생리적인 생체정보



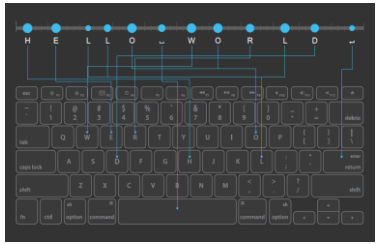
행위적인 생체정보

행위 기반 데이터를 통한 위협분석





로그인 시간의 이상 분석

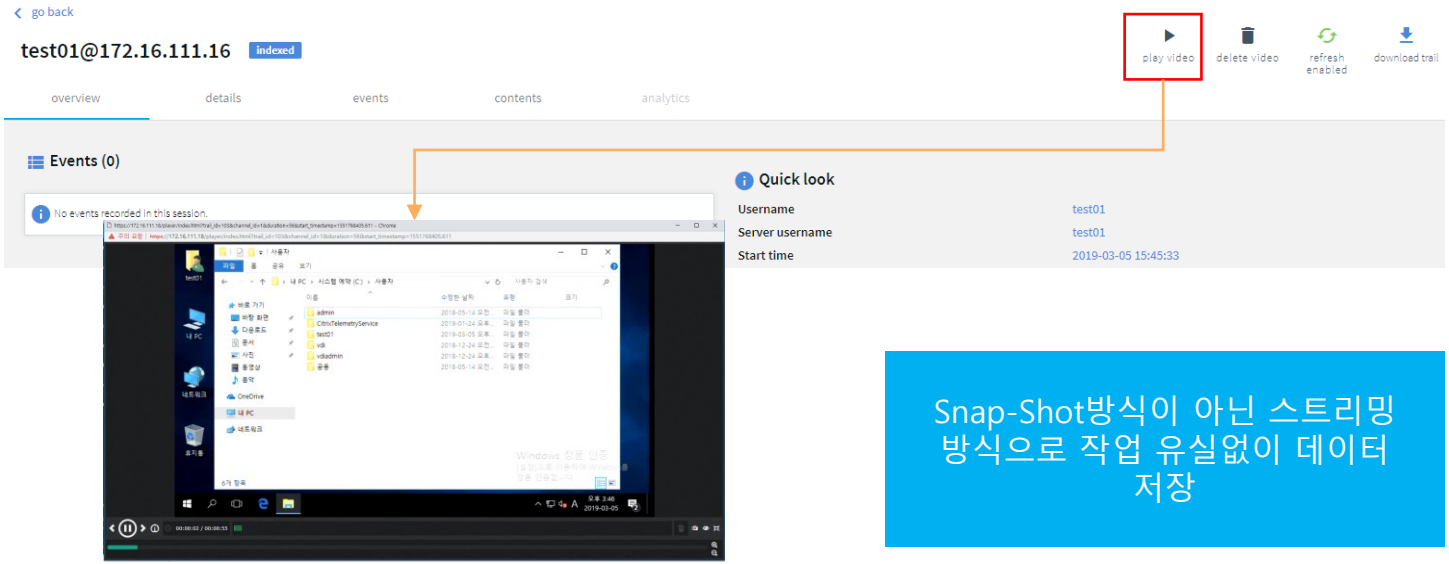


키보드 입력의 패턴 분석

마우스 이동의 패턴 분석

완벽한 녹화 기능 제공

스냅샷이나 단말에서의 녹화가 아닌 Proxy Gateway 방식으로 스트리밍 녹화



Snap-Shot방식이 아닌 스트리밍 방식으로 작업 유실없이 데이터 저장

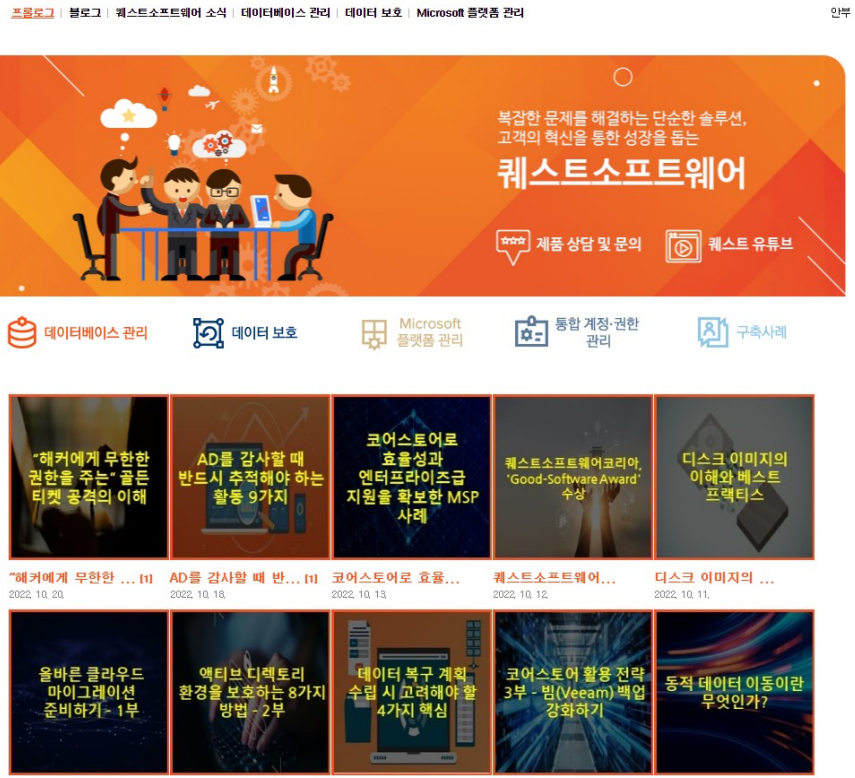
Quest

Where Next Meets Now.

Quest 블로그

퀘스트 블로그에 방문하시면
퀘스트 솔루션들에 대한 다양하고 유익한
정보를 확인 하실 수 있습니다.

URL : https://blog.naver.com/quest_kor



Quest

Where Next Meets Now.


Thank You
Quest
Where Next Meets Now.