

어플리케이션 접근통제를 통한 계정 침해 보호 및 AD 계정 침해 탐지전략

Solution Consultant / Hongso Chae

hongso.chae@quest.com

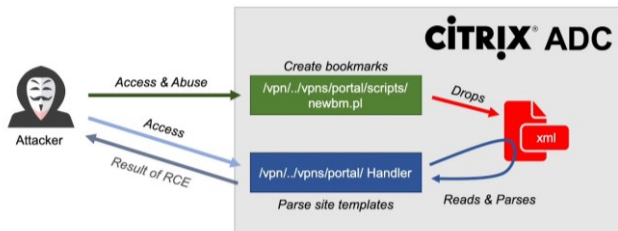
Quest

Where Next Meets Now.

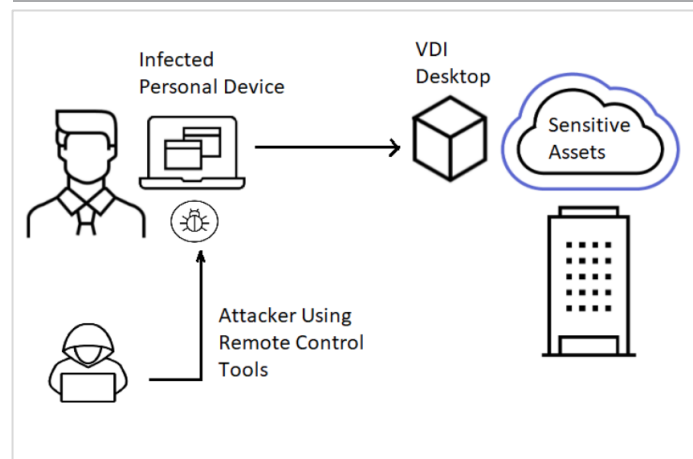
VDI 기반 재택근무 환경의 보안 이슈

취약점을 이용하여 Citrix 서버 공격

CVE-2019-19781 Exploit Sequence



개인단말 을 공격하여 내부로 접근

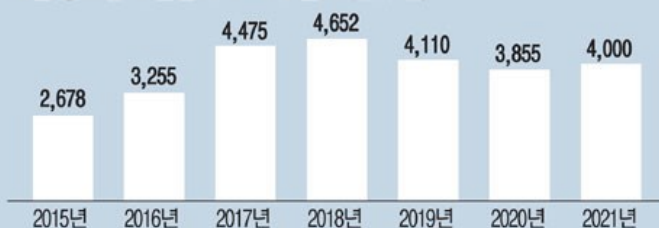


증가하는 보안 이슈

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 신고문 집계한 것

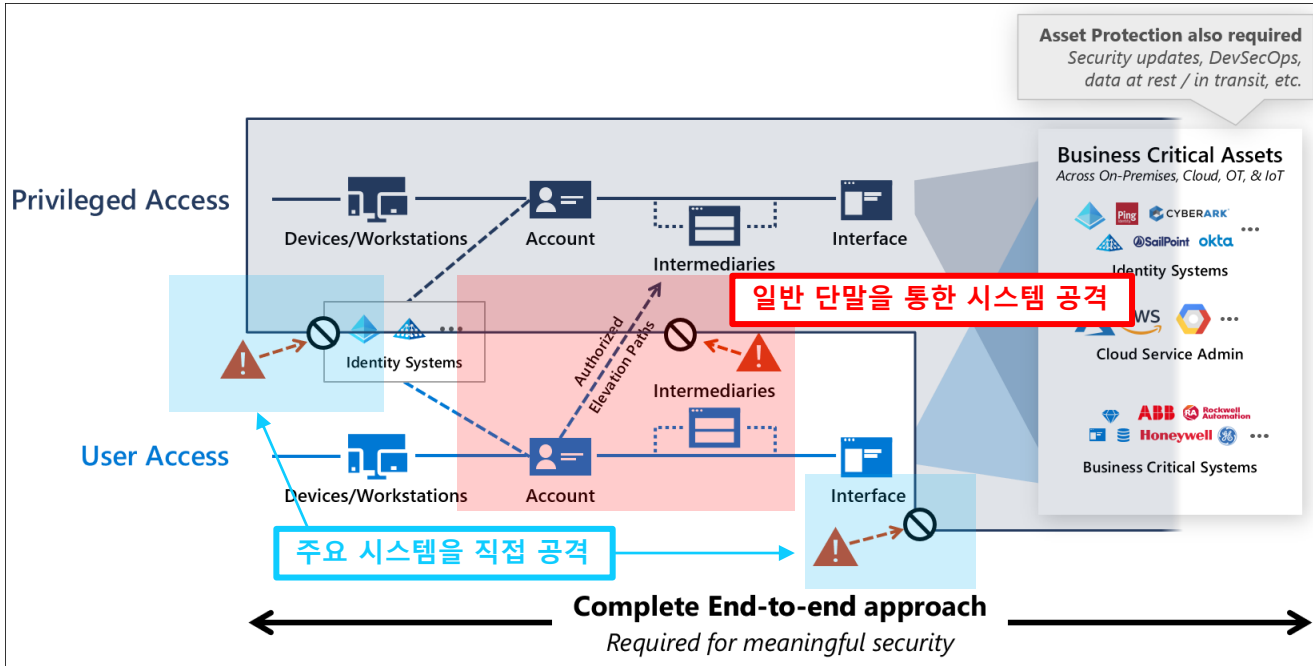


많은 보안 위험이 단말에서 발생

(재택근무가 증가하면서 이러한 보안 이슈도 증가)

이러한 환경의 변화와 증가하는
보안위협을 대응하기 위해서는
고도화된 내부 보안체계가 필요

주요 위협 접근 경로



공격의 핵심은 **계정과 권한**

일반 단말을 통한 시스템 공격

➔ Active Directory

주요시스템을 직접 공격

➔ 접근통제

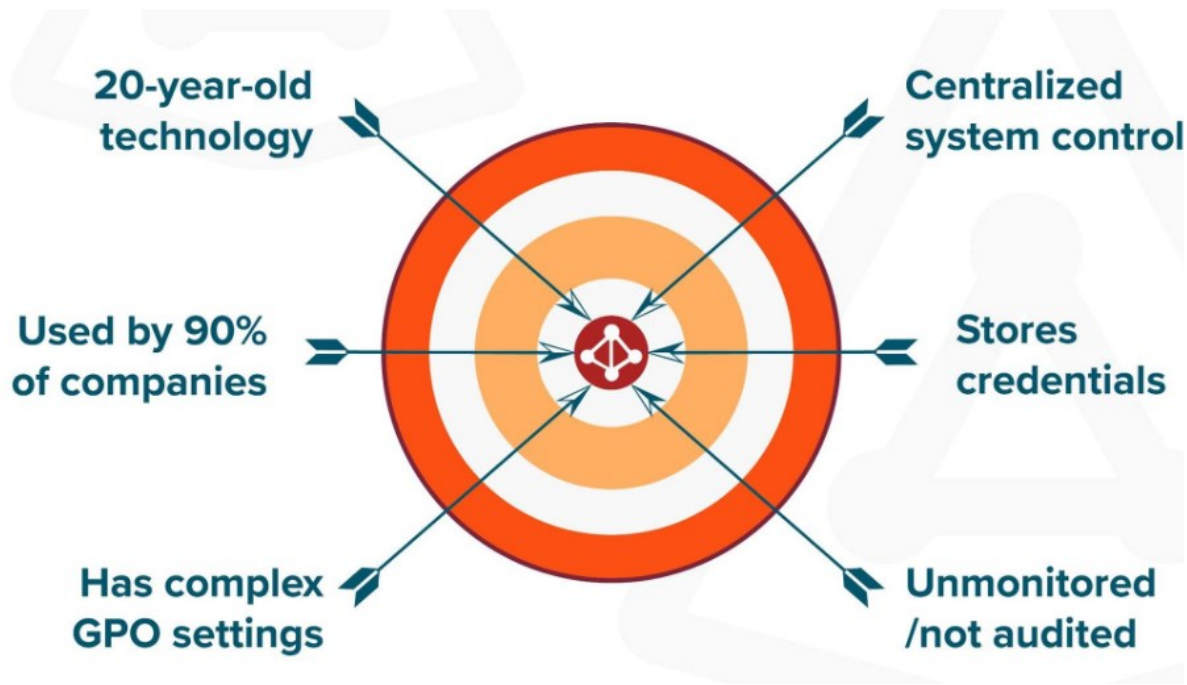
Privileged Access Strategy



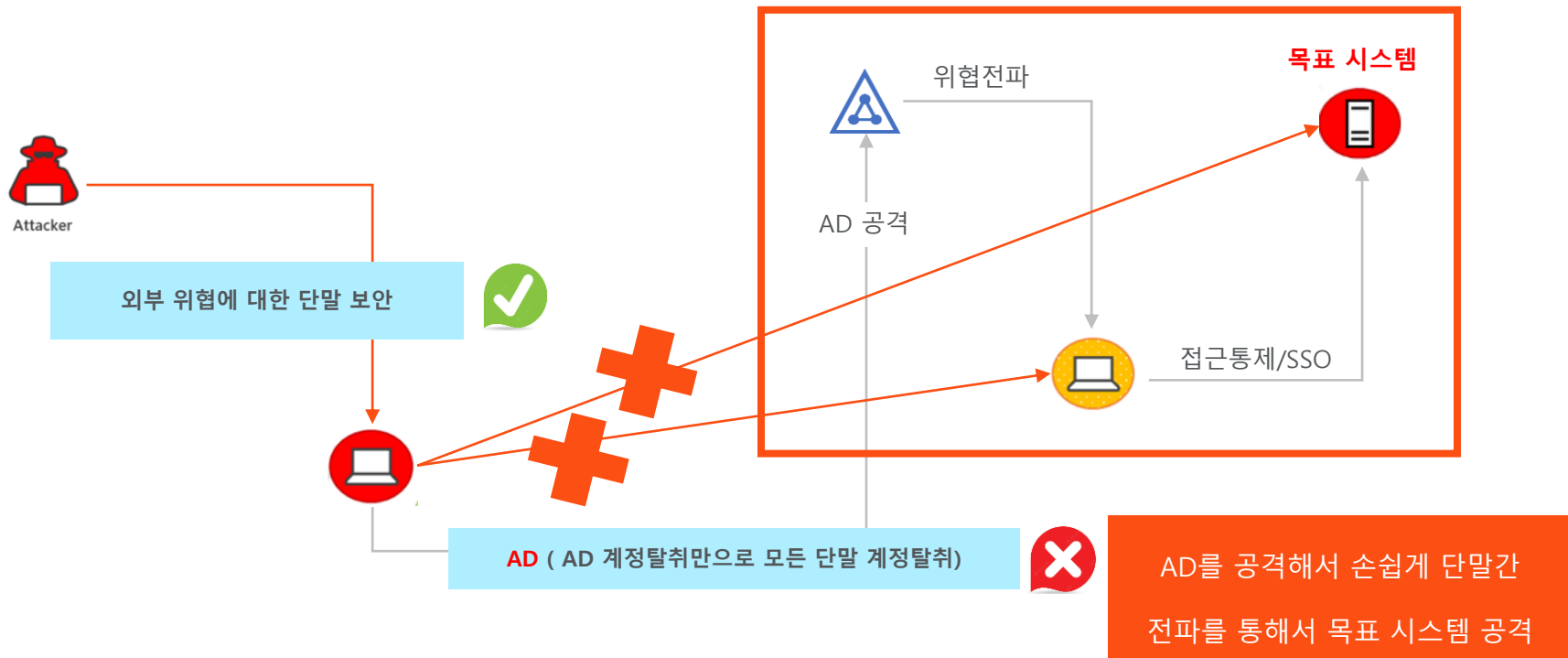
Where Next Meets Now.

Active Directory 보안이 되지 않으면?

AD는 Tier 0의 서비스로 주요한 공격 타겟



AD보안이 되지 않으면?



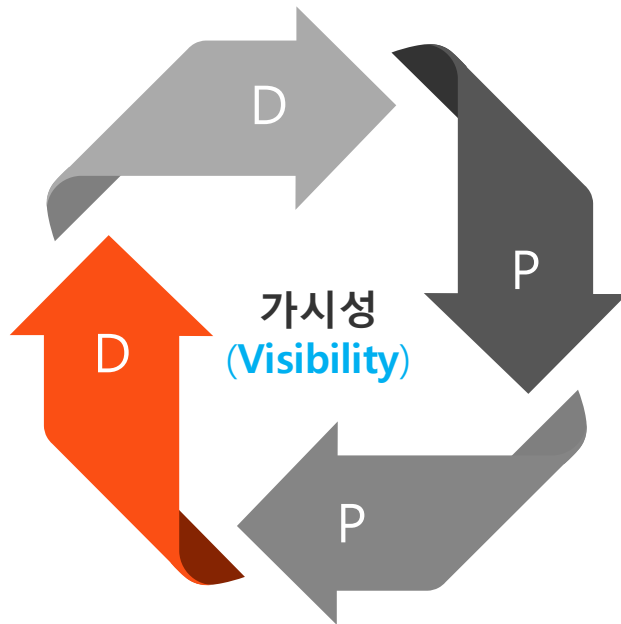
AD 보안전략(2P2D)

Diagnostic(분석)

운영과정에서의 분석 및
위험발생에 대한 원인분석을
위한 데이터 및 검색 체계

Detect(탐지)

AD에 알려진 위협 등을
통한 공격을 실시간으로
탐지하여 피해를 최소화



Prevent(예방)

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

Protect(보호)

위협이 될 수 있는 요소를
보호하여 위협요소 사전
차단

AD 복구의 이슈 발생 사례



Maersk

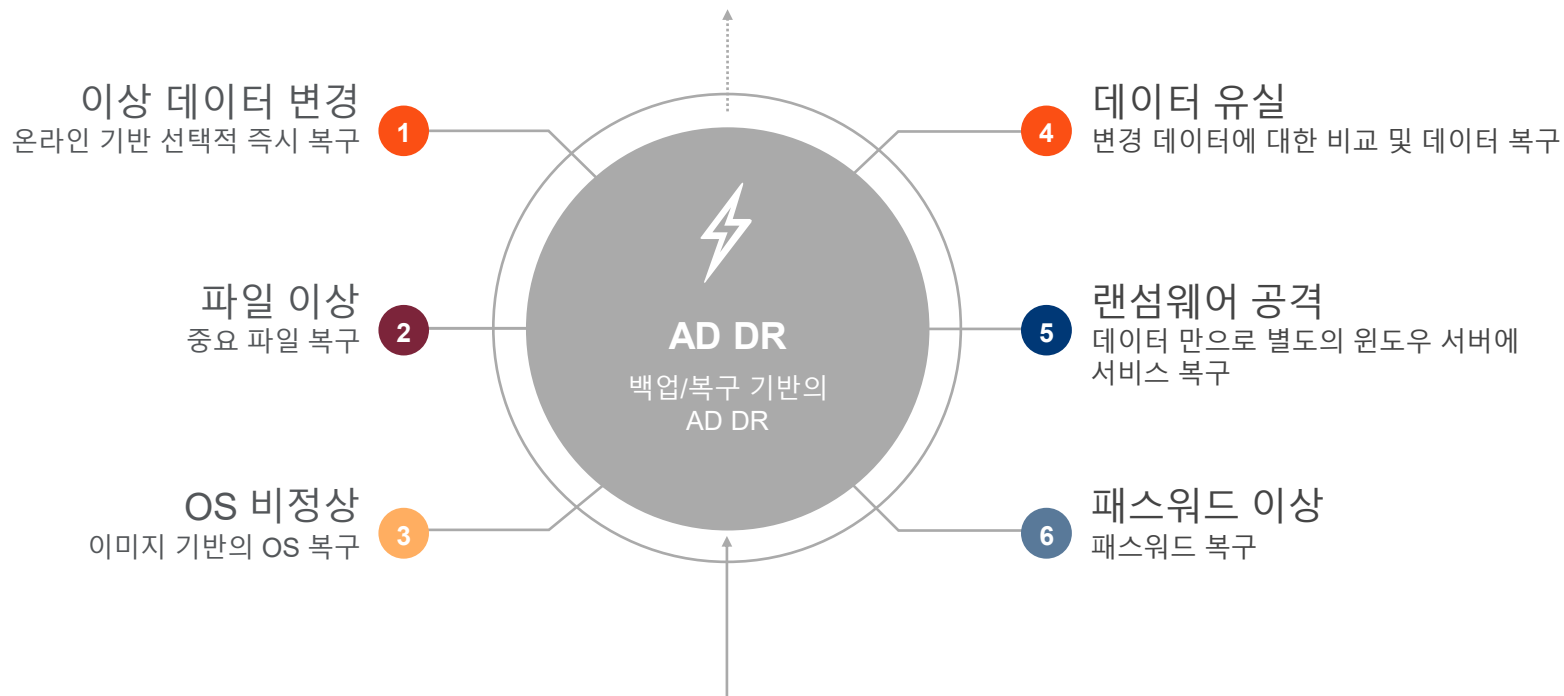
- NotPetya로 150개 DC중 149개 유실
- AD복구에 9일이 걸림
- \$\$ Millions 손실
- 뉴스 헤드라인 장식



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?

privileged account는?

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

⚠ 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.

First ransomware-related death reported in Germany Sept 2020



root



Administrator



Directories



Service Accounts



Built-in accounts



Network Devices



root

ORACLE

SYS / SYSTEM



Automation IoT



Critical Infrastructure



PLC



Social Media



by Quest

관리의 범위?



높은 권한으로 인하여 발생하는
보안/서비스 장애를 어디까지 관리할지 ?

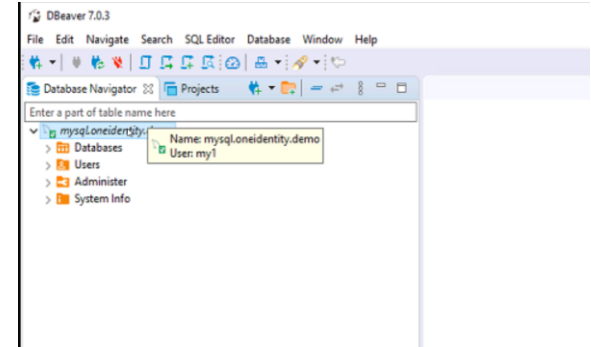
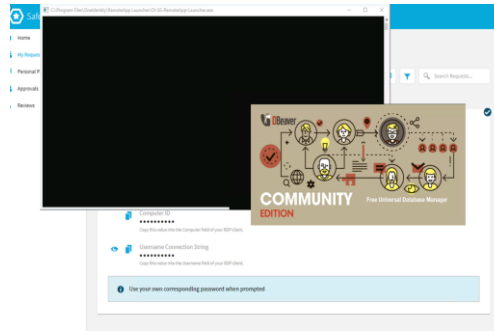
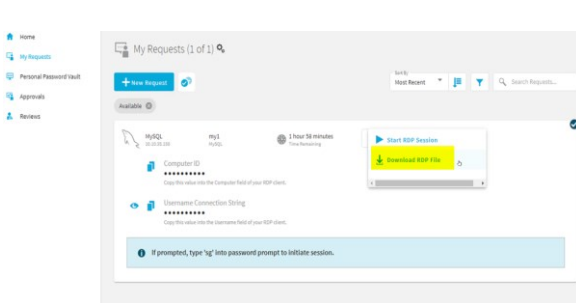
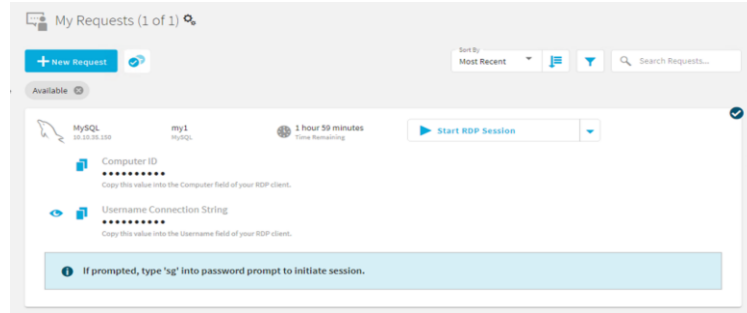
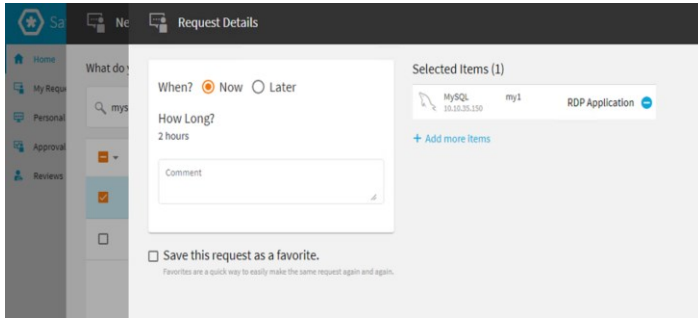
특권계정 사용자

SaaS기반의 솔루션 (Azure, AWS Cloud 포함)

The screenshot shows the 'Connect' interface. At the top, there's a blue header with the 'Connect' logo and navigation tabs for 'Connectors', 'Collaborators', and 'Logs'. Below the header, the 'Active Connectors' section features a search bar and a 'Show All' button. A single connector, 'Azure AD SG-Connect', is listed with a 'COPY SCIM' button. The 'Connector Catalog' section below has another search bar and a grid of various SaaS connectors, each with a 'CONFIGURE' button. The connectors include ActiveCampaign, Aha!, Amazon S3 AWS, Apigee, AppDynamics, Atlassian JIRA Confluence, AWS Cognito, Azure AD, Box, Citrix ShareFile, Concur, and Coupa. A 'LOAD MORE' button is at the bottom right of the catalog.

The screenshot shows the 'Asset Management' interface. On the left is a blue sidebar with navigation options: Home, Toolbox, Accounts, Account Groups, Assets, Asset Groups, Discovery, Entitlements, Partitions, Settings, Users, and User Groups. The main content area is titled 'Asset Management' and shows a list of 'Registered Connectors'. A table lists 'Azure AD SG-Connect' and 'Azure AD 1.0' with a column for 'Visible To Partitions' set to '*All Asset Partitions'. A 'Registered Connector' dialog box is open, showing configuration options for 'Azure AD SG-Connect', including 'Registered Connectors *', 'Starting Connector Version *' (1.0), 'Display *' (Azure AD SG-Connect), and a checked 'Visible To All Partitions' option. The dialog also includes 'OK' and 'Cancel' buttons.

어플리케이션(웹, C/S) 접근통제



어플리케이션 접근통제 및 행위기반 위협분석 및 녹화

2가지 형태의 생체정보



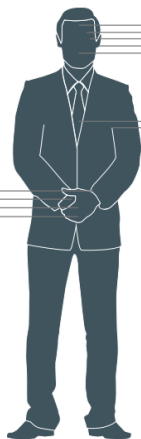
Physiological biometrics

Fingerprint recognition
Fingerprint recognition examines the small details which are found in the breaks and discontinuities located in the whorls, valleys, and ridges of the fingerprint. Although these are so distinct that even fingerprints of identical twins are different, finger scanning systems can be compromised by worn-out or cut fingerprints.

Hand geometry recognition
Hand geometry recognition examines the geometrical features of the hand. This includes analyzing the shape, and lengths and widths of the fingers.

Palm print recognition
Palm print recognition is based on the same approach as fingerprint and hand geometry recognition. Human palms also contain ridges and valleys, but these are much larger, requiring larger image capture systems. Palm prints are especially popular in forensics, as latent palm prints can often be found at crime scenes.

Vein pattern recognition
Similarly to retina recognition, vein pattern recognition identifies the pattern of blood vessels just underneath the palm or the fingertip.



Facial recognition
Facial recognition examines the distances between the most important features of the face, including the eyes, eyebrows, nose, lips, and chin.

Retina recognition
Retina recognition is based on the identification of the pattern of blood vessels which form the retina going into the optic nerve. It is frequently confused with iris recognition.

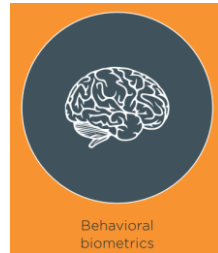
Iris recognition
Iris recognition systems examine the vector orientations of furrows and freckles in the iris. Each iris is unique and even irises of identical twins are different. Furthermore, it is extremely difficult to surgically tamper its feature information and is easy to detect artificial irises (for example, designer contact lenses). Iris recognition systems can be compromised by aging irises.

Earlobe recognition
Very similar to hand geometry recognition, it examines the distances between the prominent landmarks of the ear, as well as other unique features.

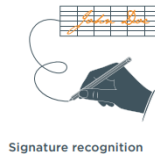
Voice recognition
Voice recognition examines the changes in the inflections and pitch in one's voice, as he or she speaks. Speech-based features are sensitive to several factors such as background noise or the emotional state of the speaker.

DNA
The DNA is the blueprint for the design of the human body. It is one of the most reliable forms of personal identification. It is intrinsically digital, and does not change during a person's life. It can be easily obtained from body fluids, nail and hair. On the other hand, DNA analysis is not only time-consuming – it requires at least 4 hours, but very expensive as well. Moreover, twins can't be distinguished by their DNA.

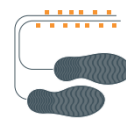
Odor/scent recognition
This experimental technology is based on the fact that there are recognizable patterns of each person's body odor that remain steady.



Behavioral biometrics



Signature recognition



Gait recognition



Mouse movement analysis

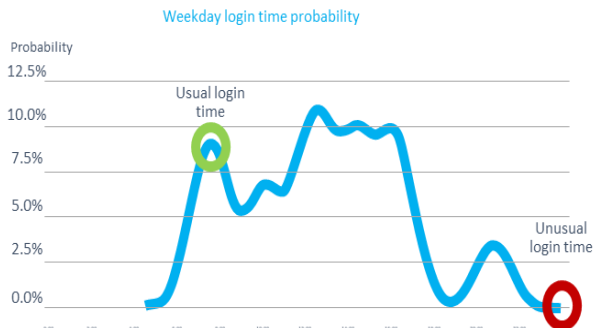
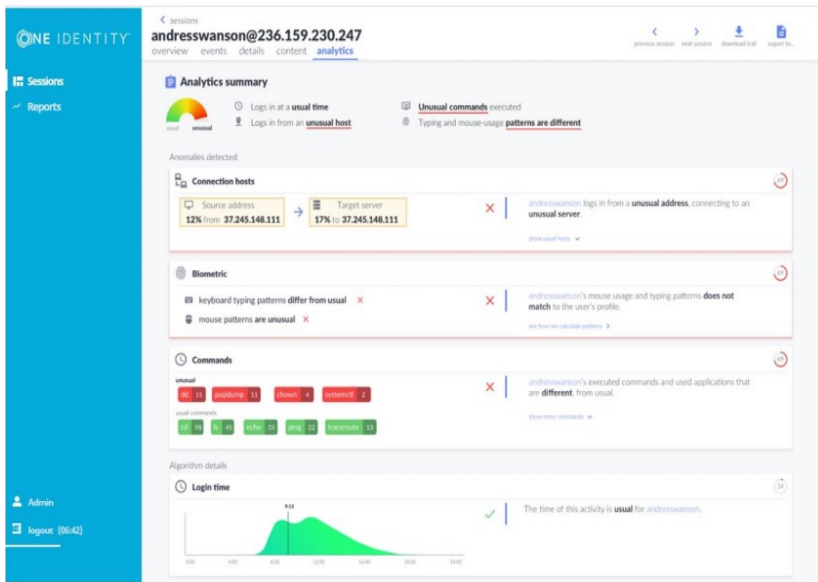


Typing rhythm

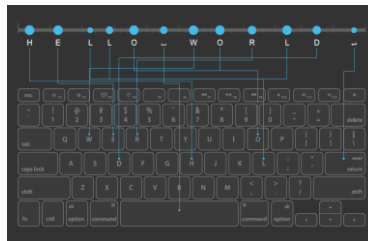
생리적인 생체정보

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

< go back

test01@172.16.111.16 indexed

overview details events contents analytics

Events (0)

No events recorded in this session.

Quick look

Username	test01
Server username	test01
Start time	2019-03-05 15:45:33

play video delete video refresh enabled download trail

Windows 인증 인증

Snap-Shot방식이 아닌 스트리밍
방식으로 작업 유실없이 데이터
저장

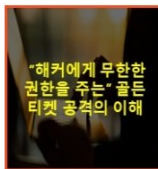
Quest 블로그

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

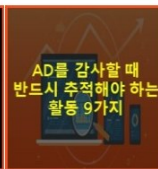
URL : https://blog.naver.com/quest_kor

프로그래밍 | 블로그 | 퀘스트소프트웨어 소식 | 데이터베이스 관리 | 데이터 보호 | Microsoft 플랫폼 관리

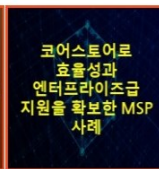
인부



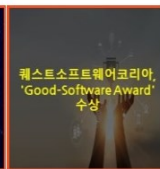
"해커에게 무한한 ... [1]
2022. 10. 20



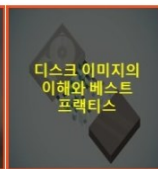
AD를 감사할 때 반... [1]
2022. 10. 18



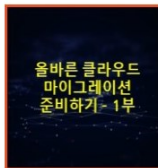
코어스토어로 효율...
2022. 10. 13



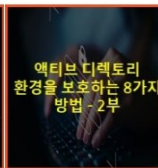
퀘스트소프트웨어...
2022. 10. 12



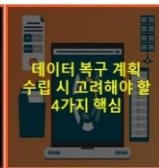
디스크 이미지의 ...
2022. 10. 11



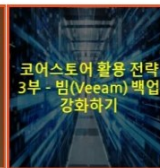
올바른 클라우드
마이그레이션
준비하기 - 1부



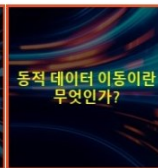
액티브 디렉토리
환경을 보호하는 8가지
방법 - 2부



데이터 복구 계획
수립 시 고려해야 할
4가지 핵심



코어스토어 활용 전략
3부 - 빔(Veeam) 백업
강화하기



동적 데이터 이동이란
무엇인가?



Where Next Meets Now.



Thank You