편리하고 안전한

ZTA기반의 재택근무 접속 과 위협탐지 전략

Solution Consultant / Hongso Chae

hongso.chae@quest.com

Quest

Where Next Meets Now.


재택근무 현재는?
Quest
Where Next Meets Now.

주요한 위협과 컴플라이언스

[재택근무에 따른 주요 보안 위협 (출처 : 美 NIST)]

구 분	주요 보안 위협
외부 단말기의 물리적 통제 미흡	- 재택근무에 사용되는 외부 단말기의 분실·도난이나 타인의 정보 훔쳐보기 시 단말기 內 데이터가 유·노출 - 외부 단말기를 통한 허가되지 않은 내부 네트워크 접근
안전하지 않은 네트워크 사용	- 공용 유무선 네트워크를 통해 내부망 접속 시 도청, 중간자 공격(MITM) 등으로 중요정보가 유출
악성코드 감염에 따른 네트워크 침해	- 악성코드에 감염된 외부 단말기로 내부 네트워크 연결 시 시스템 침해 가능
내부 자원의 원격접근 위협	- 내부에서만 접근 가능했던 내부 자원에 외부 단말기도 접근 가능해짐에 따라 비인가 접근 등 보안위협

AGR-보-2020-금-203

금융회사 재택근무 보안 안내서

2020. 12.

금 융 보 안 원

본 안내서는 전자금융거래 법령에 따른 재택근무 시 금융회사 등이 고려해야 할 보안 고려사항을 구체적으로 안내한 것으로 안내서에 대한 질의가 있으면 금융보안 레그테크 웹페이지(regtech.fsec.or.kr)의 자문 서비스를 통해 문의

보안 위협들 과 사고 사례

원자력연구원의 해킹 통로 전락한 VPN, 공공기관 취약점 점검 나섰다

출처 : 보안뉴스

한국의 경제뉴스통신사 - NSP통신 인쇄 확대 축소

[특별기고]VPN 해킹도 일상화 우려...이제 대안을 생각 할 때

출처 : NSP통신

"기업 10곳 중 6곳은 재택근무 보안 '미흡'"

최은정 기자 입력 2021.10.19 10:05

> 네트워크 접근·보안 등이 주요 고려사항으로 꼽혀

출처 : 아이뉴스

앞으로는..

기업 10곳 중 4곳, 위드 코로나에도 재택근무 유지할 것

잡코리아 | 2021-10-05 14:39 | 1,140

출처 : 잡코리아

Quest

Where Next Meets Now.


가장 큰 보안 위협은
통제되지 않는 외부 단말
Quest
Where Next Meets Now.

통제되지 않은 단말이 최대 위협

- 허가 받지 않은 사용자 접근
- 단말로부터의 데이터 유출
- 외부 단말로부터의 내부 접근

단말 위협의 형태

단말 위협

- 외부단말의 해킹 또는 분실

비인가 위협

- 허용되지 않은 사용자의 접속
- 허용된 사람이 연결해 놓은

세션을 통한 공격

위협내부 전파

- 재택근무 단말을 통한 위협이 내부 전파

위협 대응 방안

Quest

Where Next Meets Now.

단말 위협

주요 대응 방안과 한계

주요 대응 방안

- 단말 로그인 강화(2FA)
- 단말 보안제품 설치
- 최신 보안 패치 유지
- 데이터 암호화(BitLocker)
- 전용 단말 지급

현실적인 한계

- 단말 지급을 위해서 별도의 비용 발생

- 지급된 단말 관리의 어려움
- 보안제품이 정상적으로 동작하는지 확인 어려움
- 단말 보안제품에 대한 관리 어려움
- 최신 패치를 지속적으로 관리하기 어려움
- OS/VPN등의 소프트웨어 취약점

- 모든 위협에서 단말을 완벽히 보호하기는 어려움

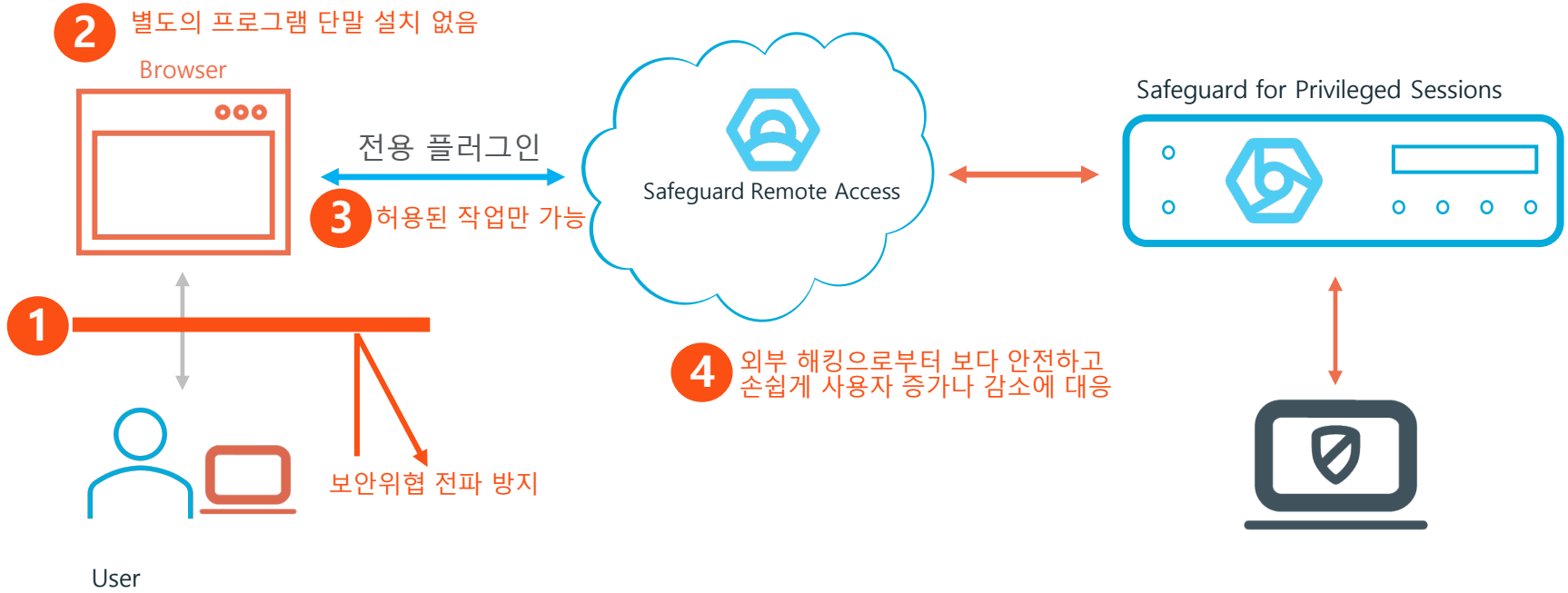
단말 위협을 대응하는 최선 보안방안

단말은 언제든 위협에 노출될 수 있다는
가정하에
안전한 접속방식 제공

전용 단말 지급과
보안제품을 통한 단말
보안강화는 선택

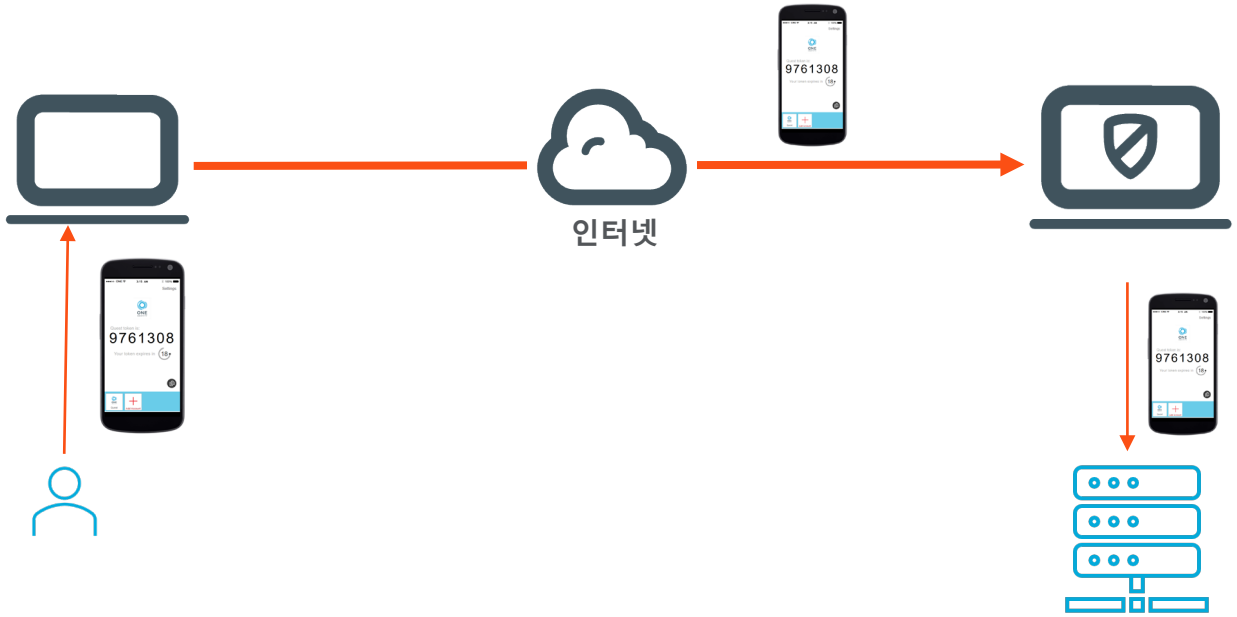
현재 이것을 제공하는 대표적인 방식이 VDI

퀘스트는 어떤 방식을 제공



비인가 위협

비인가 접근을 막는 최선은 **MFA**

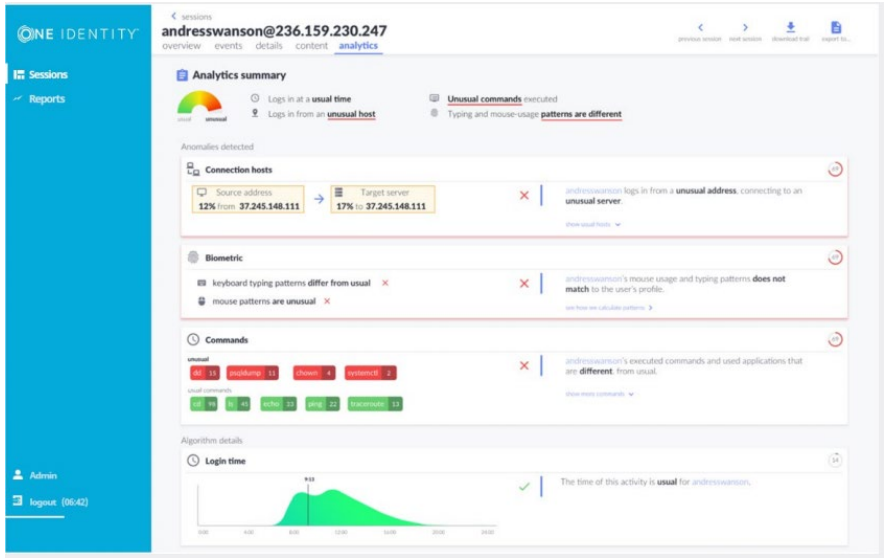


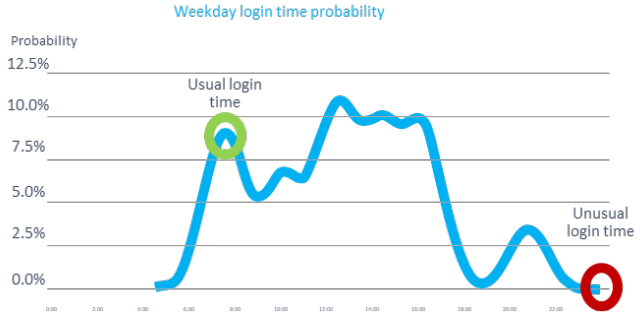
Quest

Where Next Meets Now.

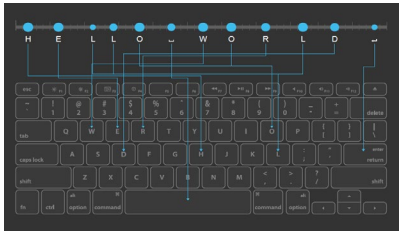
그렇다면 연결된 세션을 통한 위협은?

연결된 세션에 대한 공격은 크게 행위 기반 분석을 통해서만 대응





로그인 시간의 이상 분석



키보드 입력의 패턴 분석

마우스 이동의 패턴 분석

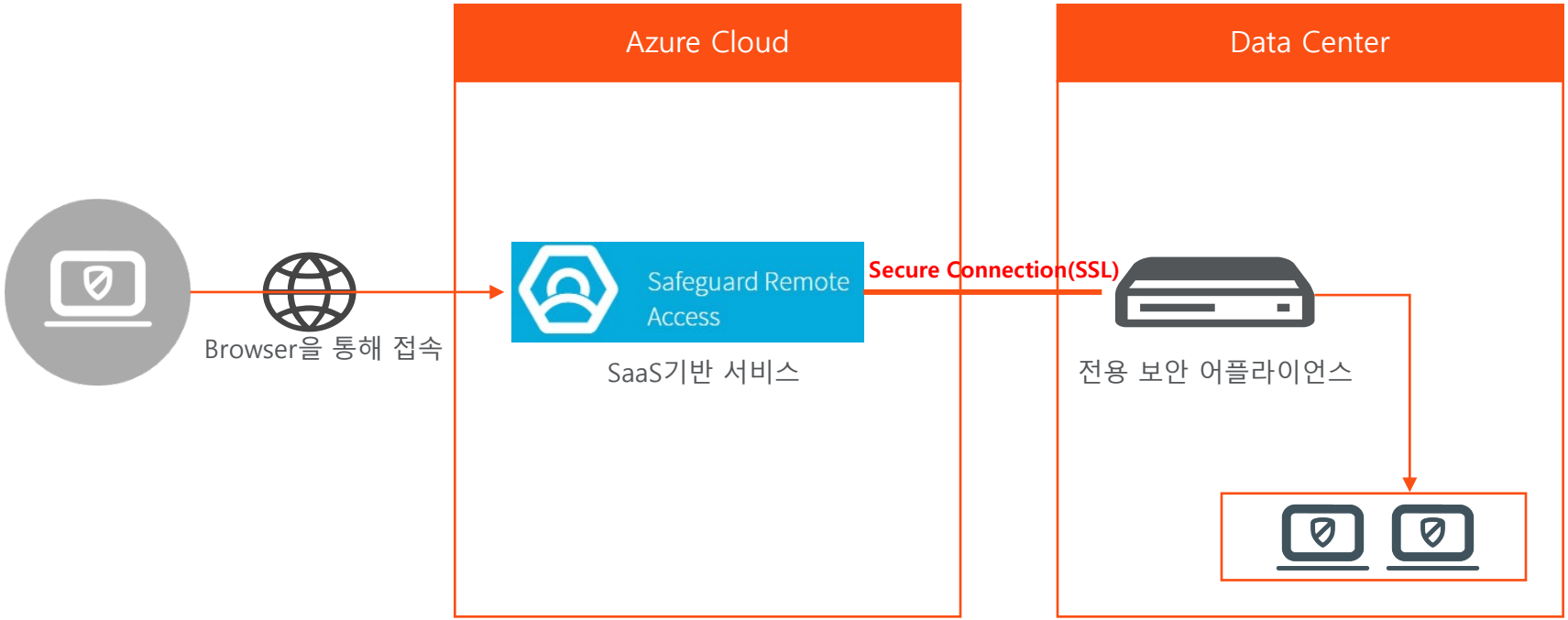
Quest

Where Next Meets Now.

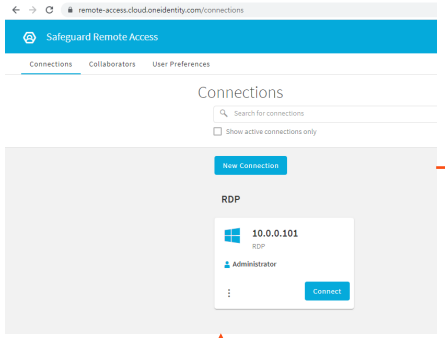
Quest 솔루션은?

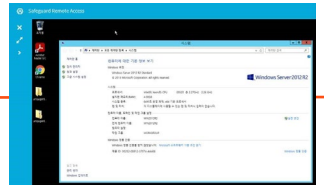
Quest
Where Next Meets Now.

구성


Azure Cloud
Data Center
Browser을 통해 접속
Safeguard Remote Access
SaaS기반 서비스
Secure Connection(SSL)
전용 보안 어플라이언스

재택근무 환경에서의 접근 흐름

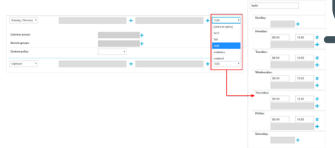




행위기반 ML을 통한 위협 분석

모든 접근 행위 녹화 및 실시간 확인

모든 접근내역 데이터화



시간대별 접근 통제등의 접근 통제

사용자 단말 위협이 시스템 내부로 전이되지 않음

Quest

Where Next Meets Now.


그렇다면 이렇게 하면 보안위협 대응이 완벽한가?
완벽하지 않다고 생각한다면,
내부탐지 체계의 고도화가 필요하다.
Quest
Where Next Meets Now.

내부위협 탐지 체계의 고도화 (잠재적인 위협 요소)

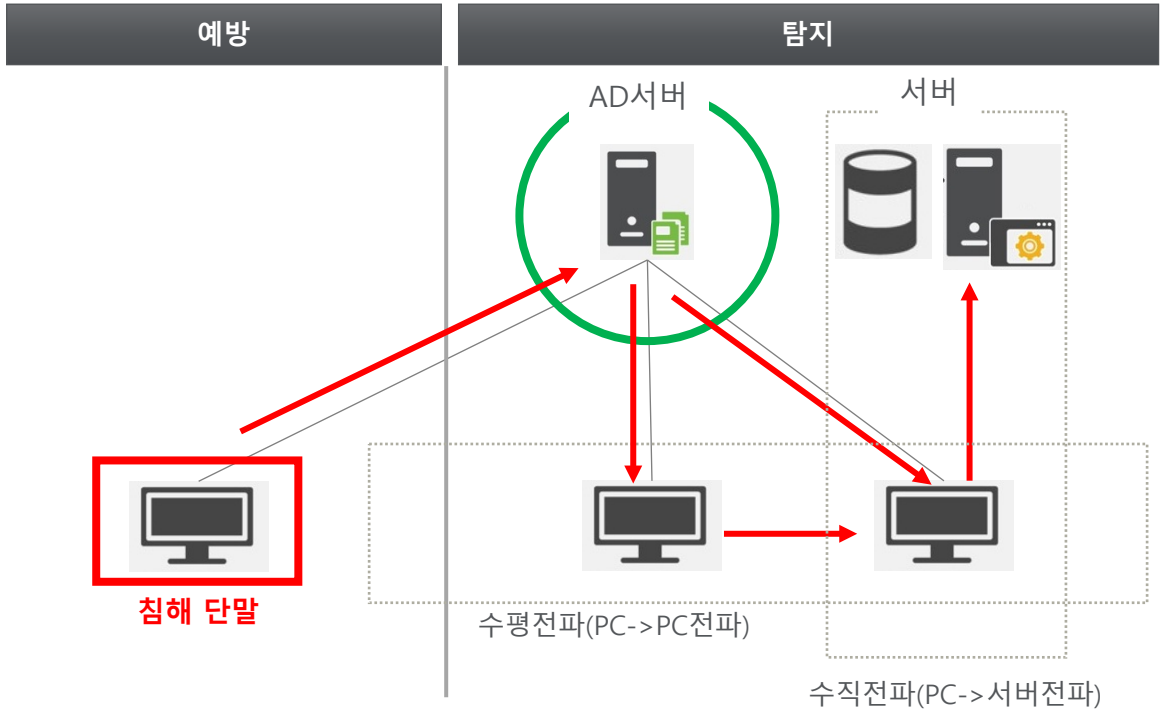
Quest

Where Next Meets Now.

단말 위협의 전파

재택근무 환경에서
단말의 보안 침해의
가능성은 항상 존재

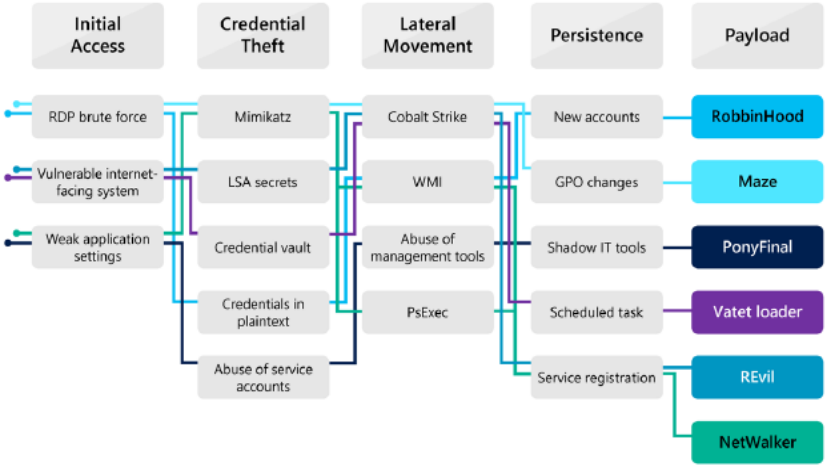
그럼 이러한 위협을
대응하기 위해서는 내부
탐지 체계 필요

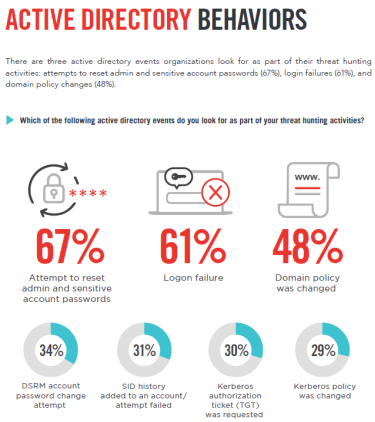


Quest

Where Next Meets Now.

AD 보안 권고





AD기반 환경의 주요한 공격대상인 GPO, 계정에 대한

모니터링 체계 구축 필요

Quest

Where Next Meets Now.

AD 보안 전략

STEP1

Protect

정책 기반 **보안체계**

- 시스템 보안
- 서비스 보안
- 계정 보안

STEP 2

Detect

가시성 기반 **실시간위협 탐지체계**

- 위협 탐지
- 정책 위반 탐지
- 이상행위 탐지

STEP 3

Recover/Response

데이터 기반 **분석 및 대응 체계**

- 위협 및 이상행위 분석
- 복구

Quest

Where Next Meets Now.

Quest 솔루션은?

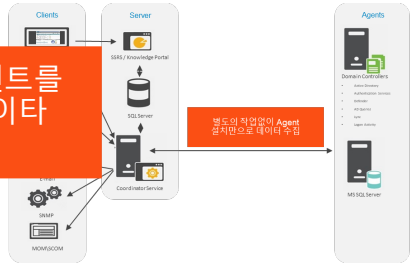
Quest
Where Next Meets Now.

데이터 기반의 실시간 위협 탐지

모든 행위 이벤트를 수집(자체 데이타 생성)

위협을 체계적으로 정의 및 탐지

글로벌/국내에서 유일하게 검증되고 다수의 구축 경험



탐지

인사정보 자동동기화(입사,퇴사,이동)

Tier0 Secure Zone

Provisioning/De-Provisioning

On-premises Active Directory

Azure AD Connect Server

Azure AD

Office 365

Your Apps

Saas Applications

Join

Windows 10

통합콘솔로 접근통로 단일화
(직접 접근 제한)

PAW(SAW)

Change Auditor

Quest

Where Next Meets Now.


Thank You
Quest
Where Next Meets Now.