AD를 통한 랜섬웨어 공격의 모든 것!

Solution Consultant / Hongso Chae

hongso.chae@quest.com

Quest

Where Next Meets Now.

Cybersecurity and Cyber Resilience

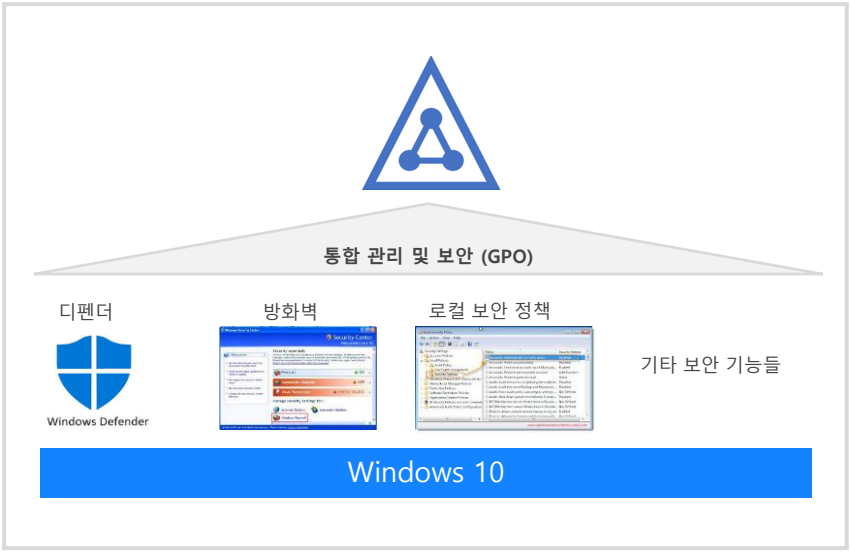
위협에 대한 대응

비즈니스의 연속성

Active Directory는 ?

단말 통합관리

단말(Windows 10, Server) 보안 및 관리



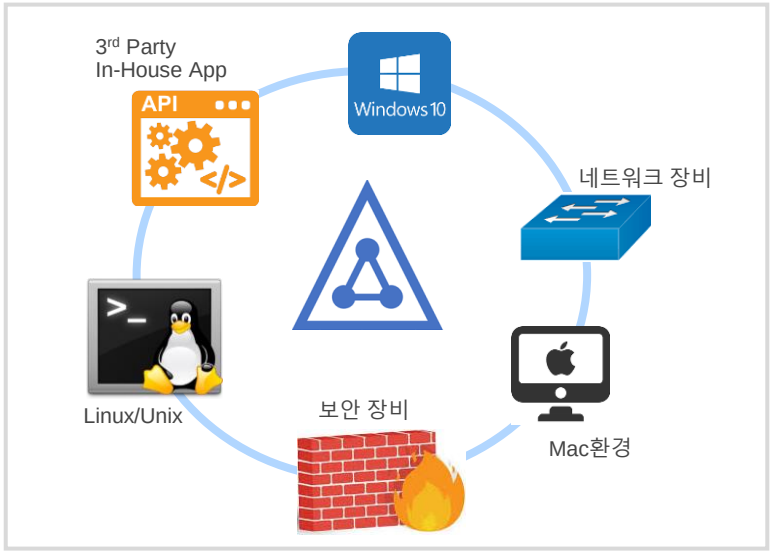
연결된 모든 장비들을 손쉽게

- 바탕화면 변경
- 브라우저에 링크를 추가
- 패스워드 정책 설정
- 방화벽 설정
- NIC/프린트 관리

Cybersecurity

통합 인증

통합인증(계정통합)



표준 인증을 지원하는 대부분의 서비스/장비에

- 통합인증
- 권한관리
- ID단위 인증

Cyber Resilience

감사

대부분의 VDI에서 AD를 통합인증으로 사용

Cybersecurity

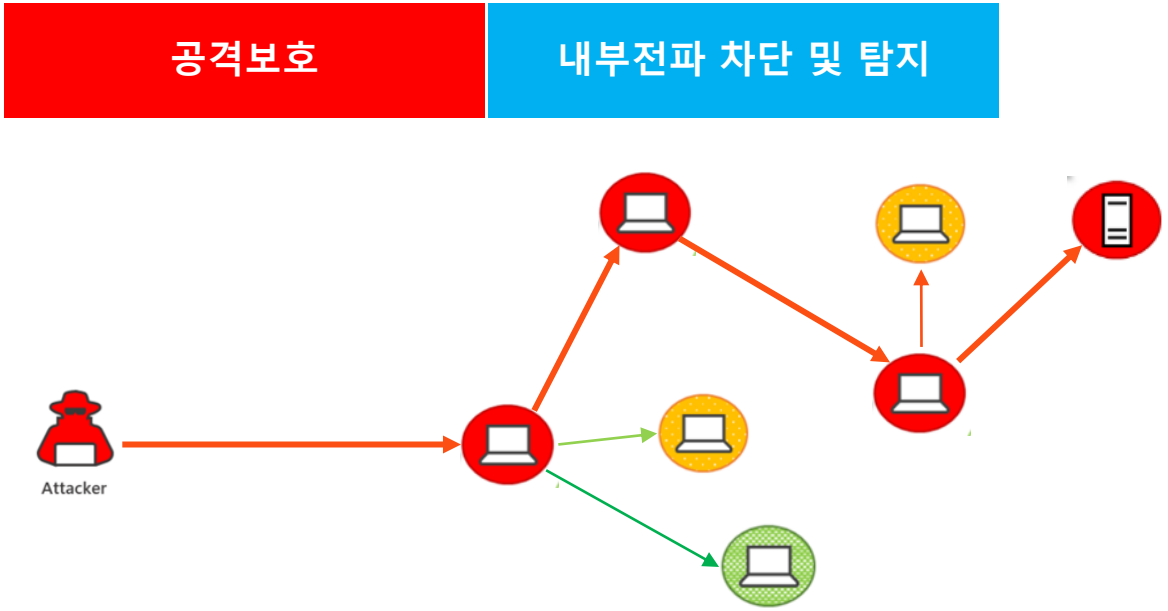
- 단말통합관리

Where Next Meets Now.

단말 보안?

단말 보안의 2가지 영역

단말 보안 = 공격으로부터의 **단말 보호** + **단말간 전파**에 대한 **차단 및 탐지**

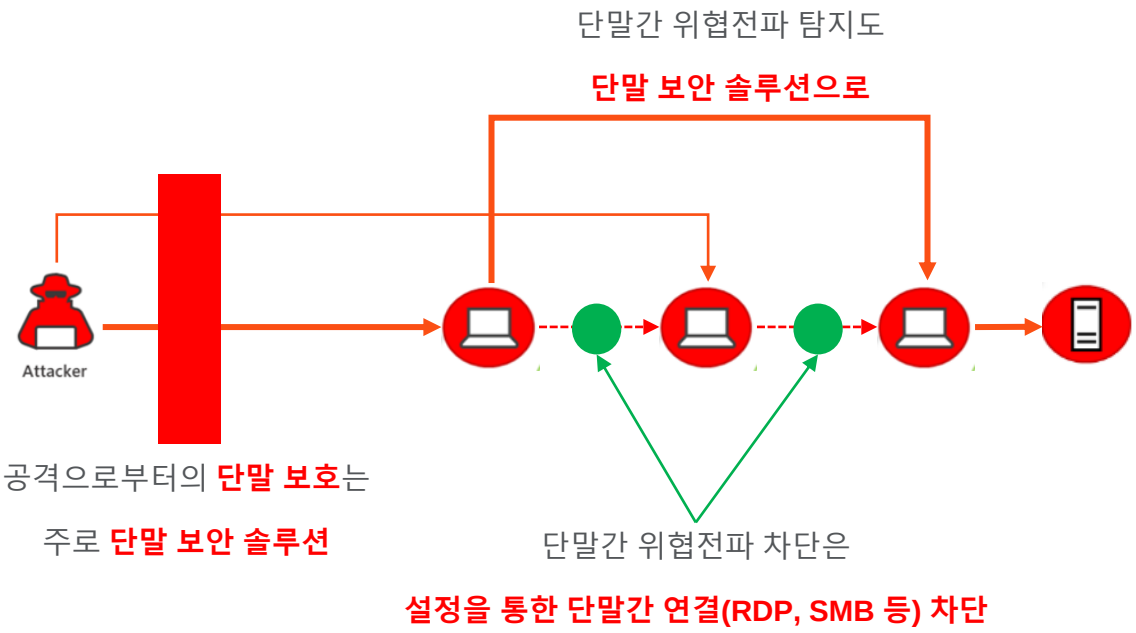


AD가 없는 환경에서의 단말 보안?

Quest

Where Next Meets Now.

AD가 없는 환경은 단말보호 솔루션으로..



단말보호 관점의 **단말 보안 솔루션**과

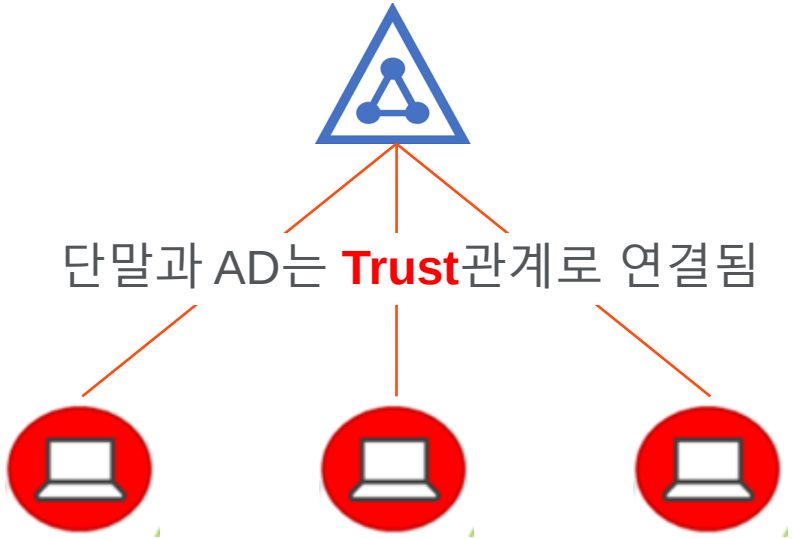
설정으로 단말 보안

AD가 있는 환경에서의 단말 보안은?

Quest

Where Next Meets Now.

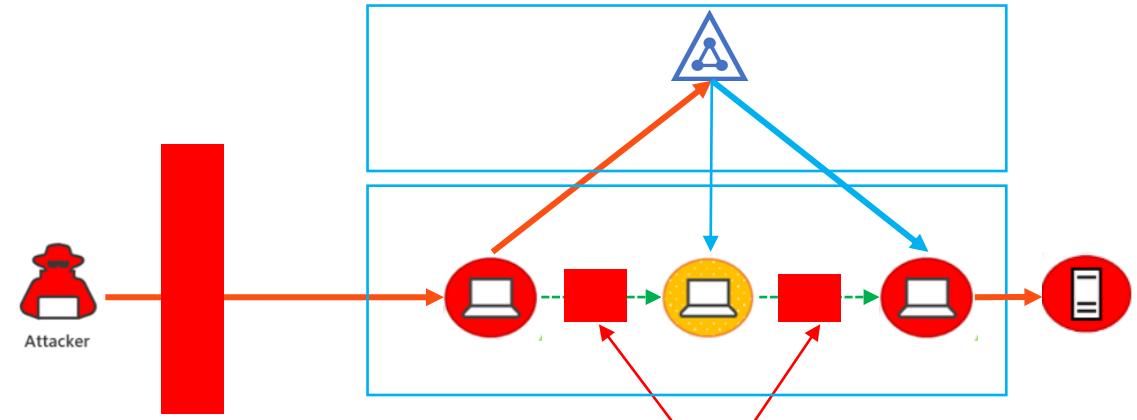
단말이 AD로 구성되어 있다는 것은?



AD 단말 환경에서의 단말보안

단말간 위협전파 차단과 탐지는

AD 보안을 통해서



새로운 AD 보안 체계

+

기존 단말보호 체계

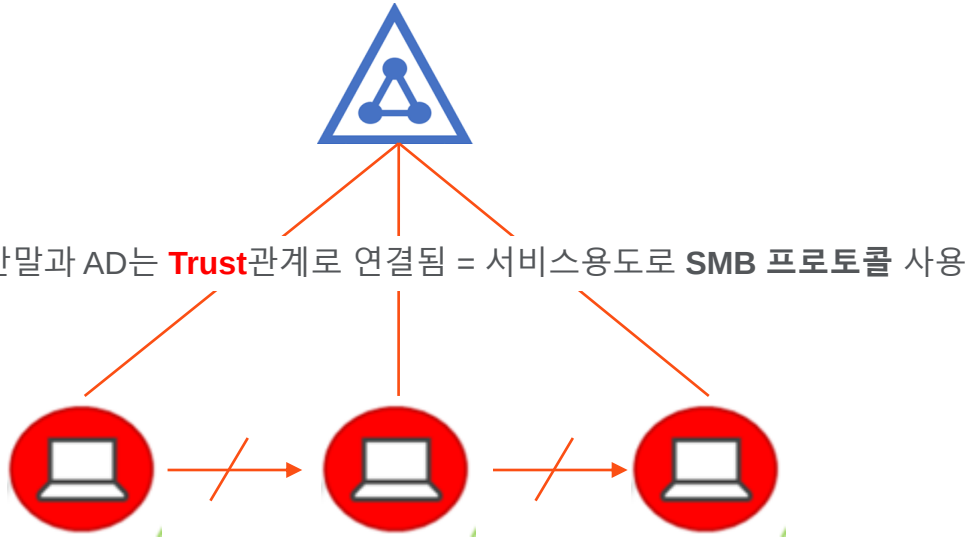
공격으로부터의 **단말 보호**는

주로 **단말 보안 솔루션**

단말간 위협전파 차단은

GPO 설정을 통한 단말간 연결(RDP, SMB 등) 차단

그런데 왜 AD를 통해서 내부 전파?



이유 #1. 단말과 AD는 **Trust**관계로 연결됨 = 서비스용도로 **SMB 프로토콜** 사용

이유 #2. 단말을 개별로 공격하는 것은 **많은 비용** 필요

- 직접 연결을 사전에 차단 : 단말간 RDP, SMB 차단
- 공격대상이 너무 많은 : 모든 단말을 개별로 공격

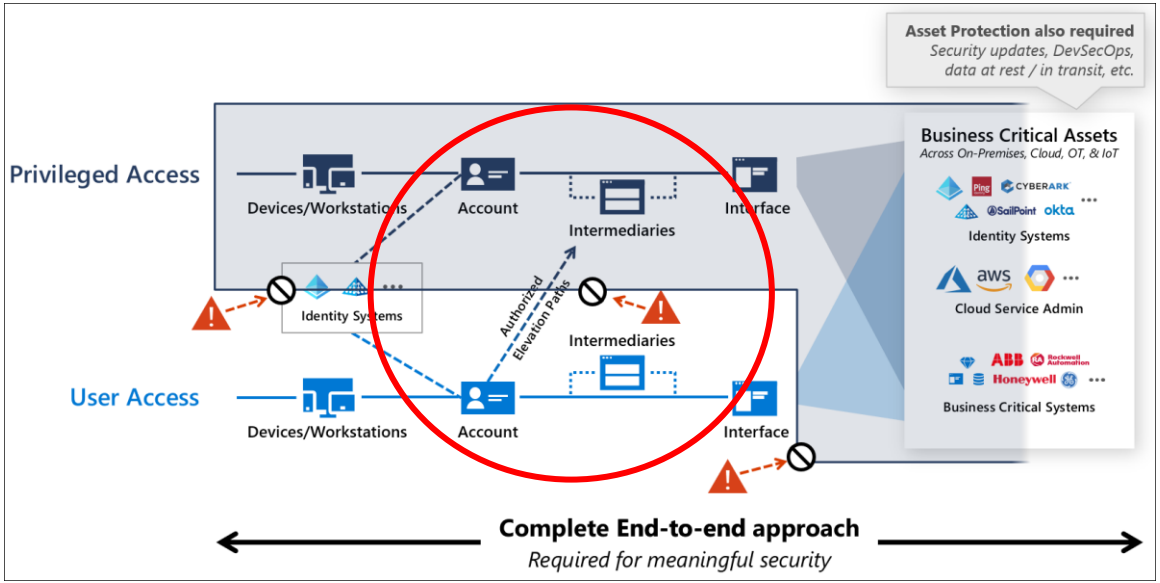
AD의 위협은?

일반 단말을 통한 공격

공격으로 탈취된 단말

(대부분 일반 단말)을 통해서 접근

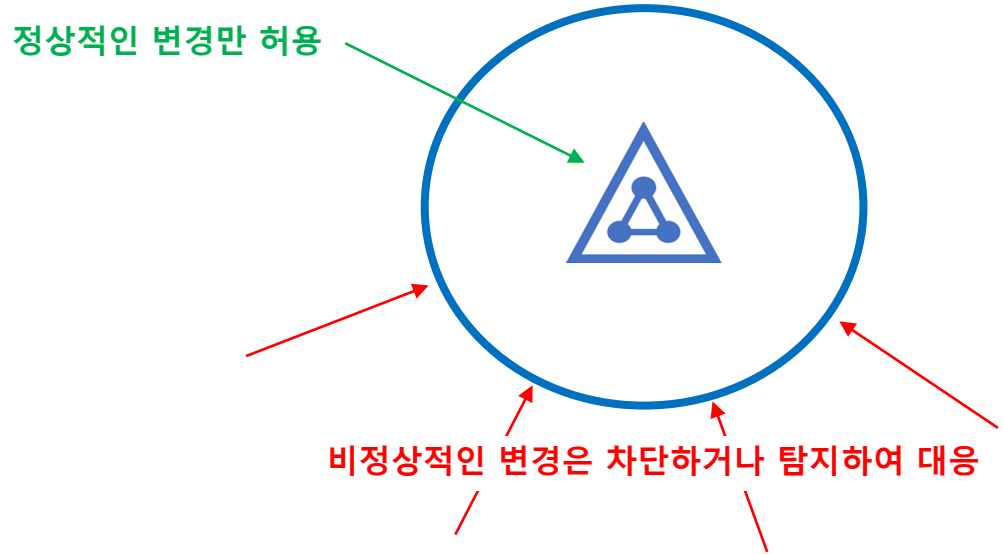
Microsoft의 Privileged Access Strategy



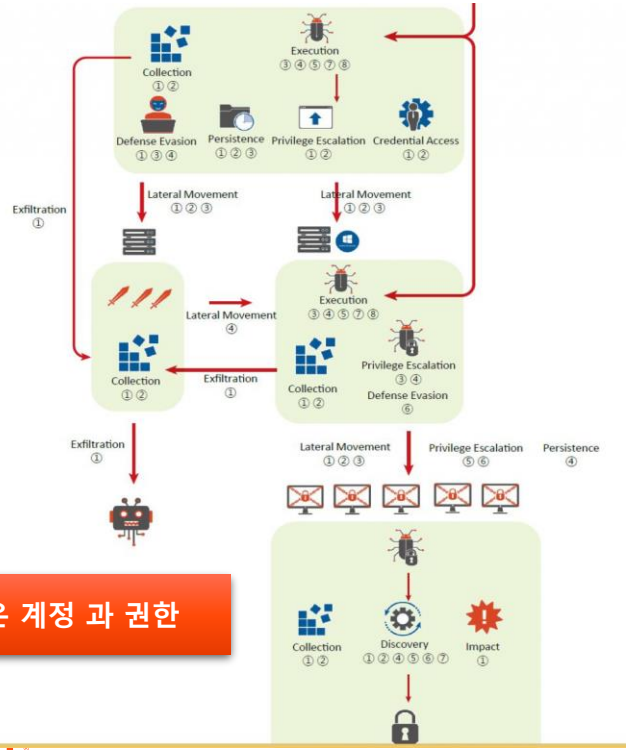
높은 권한 계정(권한) 탈취

권한 획득을 위해서는 AD의 데이터 변경 발생

(또는 어딘 가에 저장된 데이터를 획득)



핵심은 계정과 권한



핵심은 계정 과 권한

【Defender's Insight】

'한국인터넷진흥원'은 본 보고서를 통해 AD환경에서 발생하였던 랜섬웨어 감염 공격 유형에 대해 살펴보았다. 공격자는 스피어피싱을 통한 내부 침투, 계정 탈취 후 DC 서버 장악, SMB기능을 통한 내부 이동의 과정을 통해 랜섬웨어에 감염시켰다. 이러한 사고는 공격자가 요구한 대가 지불액, 기업의 이미지 손상에 따른 피해, 시스템 복구 비용 등 막대한 손실이 발생할 뿐 아니라 AD의 특성상 시스템 전체가 장악되어 기업 주요 정보 유출 등 추가 피해가 발생할 수 있다.

앞으로도 기업들을 대상으로 한 해킹사고는 끊임없이 발생할 것이고 AD를 사용하는 기업들도 타겟이 될 것이다. 기업마다 망 구성방식, 권한 관리, 보안 정책 등이 다르기 때문에 침투 방식이나 세부적인 공격 방법은 변경될 수 있으나 권한상승, 계정 탈취, SMB를 통한 내부 이동 등은 대부분의 AD사고에서 확인되는 공통적인 특성이다.

따라서 AD환경을 사용하는 기업 입장에서는 계정 관리 및 모니터링이 제일 중요하다.

최초 침투에 성공한 공격자는 관리자 계정 탈취를 목표로 내부망을 탐색하고 이동할 것이고 이때 일반 사용자 계정을 아무리 많이 탈취하더라도 내부망 장악에 도움이 되지않는다. 때문에 계정이 탈취되더라도 AD DC(Domain Controller)서버를 장악할 수 없도록 사용자 및 서비스 계정들의 권한을 분리하여 관리하여야 한다. 관리자 그룹 계정 사용을 최소화하고 불가피하게 관리자 계정을 사용하는 시스템들은 주기적으로 모니터링하여야 한다. 특히 AD DC의 경우 등록된 서비스와 그룹 정책 목록에 의심스러운 사항은 없는지 주의를 기울여야한다. 또한 주요 시스템 로그는 주기적으로 백업하고 계정 탈취 도구가 탐지되거나 파이프 통신 발견 시 즉시 전사 시스템을 점검해보아야한다.

AD 보안 전략

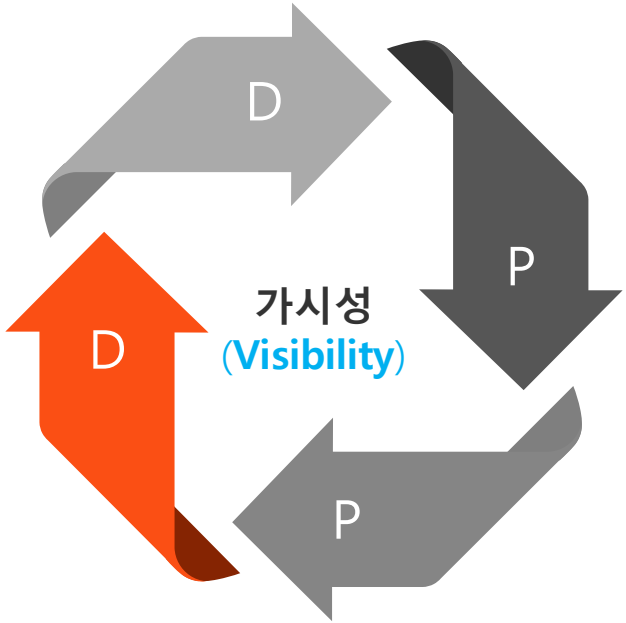
Quest

Where Next Meets Now.

AD 보안전략(2P2D)

Diagnostic(분석)

운영과정에서의 분석 및 위협발생에 대한 원인분석을 위한 데이터 및 검색 체계



Protect(보호)

위협이 될 수 있는 요소를 보호하여 위협요소 사전 차단

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

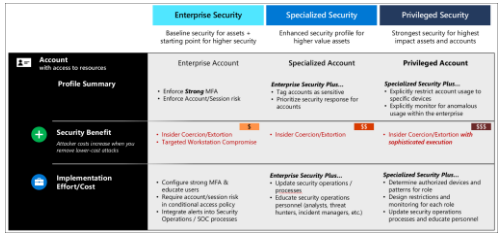
AD 보안 전략

전략 #1. 예방

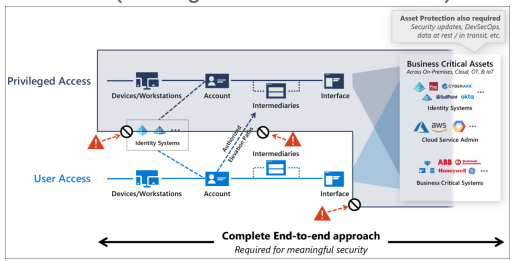
Quest

정책기반위협을 통한 예방

정책 기반 위협



PAW(Privileged Access Workstation)



Privileged Access Strategy

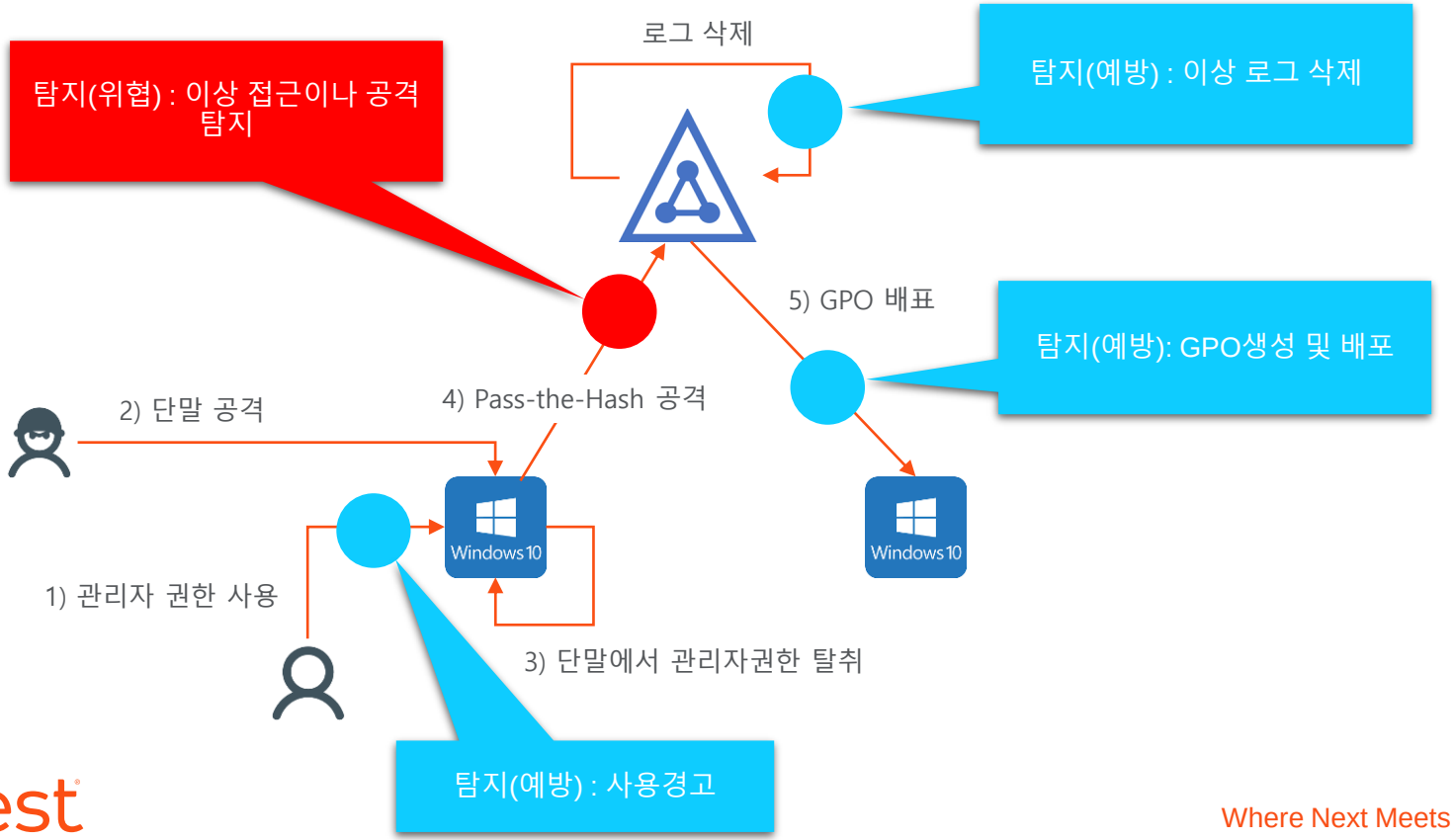
공통적인 위협

- 일반 단말에서 관리자 계정 사용
- 방화벽정책 비활성화
- 기본 Administrator 계정 활성화
- Guest계정 활성화
- 허용되지 않은 경로에서의 사용자 계정 추가

회사내부 보안정책기반 위협

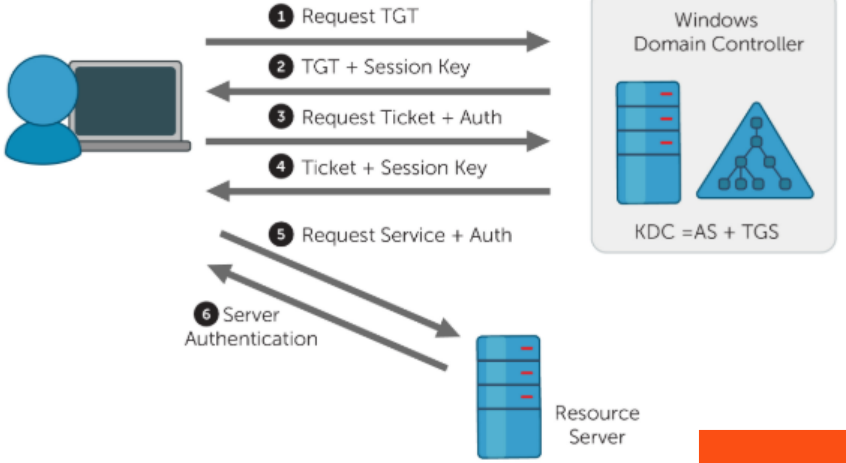
- 계정 별 허용되지 않은 작업 수행
- 허용되지 않은 위치에서의 접근(관리자권한 계정)
- 퇴직자 계정 활성화

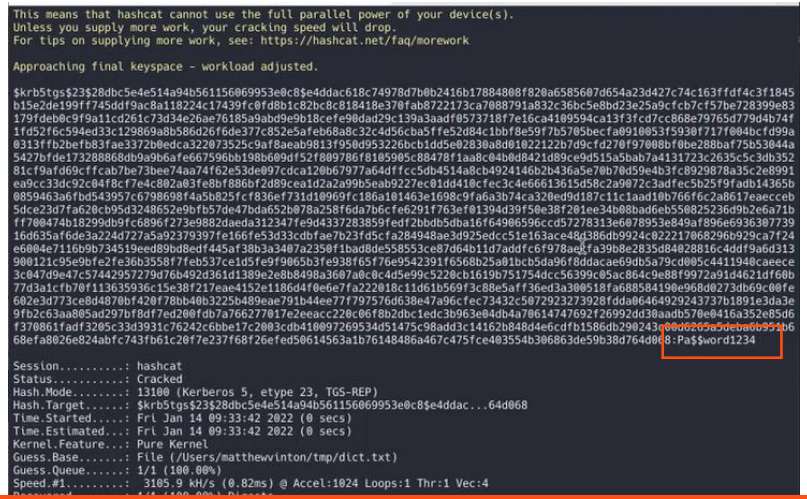
사전 탐지를 통한 위협예방 예시



사전 탐지를 통한 위협예방 사례

Kerberos Roasting 공격 : Kerberos를 통해서 계정탈취





국내 고객사에서 일부단말에서 해당 공격을 위해서 필요한

ServicePrincipalName의 비정상 변경을 확인하여 해당 공격 사전 대응

AD 보안 전략

전략 #2. 보호

알려진 위협이나 회사 보안정책 위반 보호

변경 되었을 때 영향도가 큰 변경 보호

전사 보안 GPO(Default GPO)

최상위 관리자만 작업을 할 수 있거나

변경이 되었을 때 큰 보안위협이 될 수 있는 항목

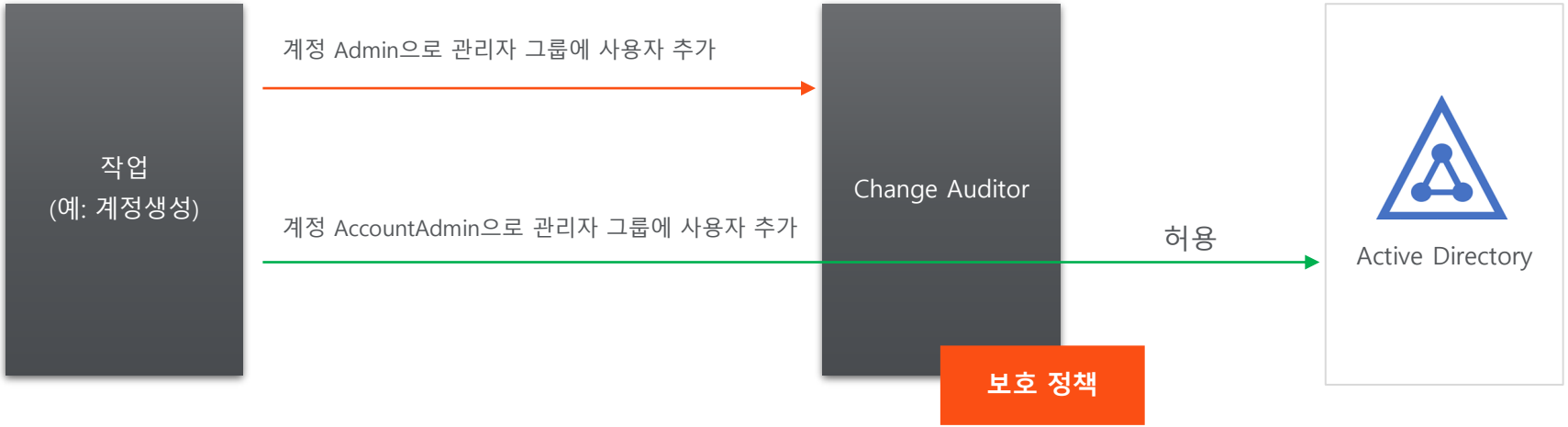
허용된 계정을 통한 작업만 보호

계정관리를 통한 사용자 추가만 허용

업무 워크플로우가 있는 형태처럼 회사내부에

이미 보안정책이 있는 경우(허용된 경로가 존재)

보호 처리방식



정책 : 관리자 그룹에 사용자 추가는 AccountAdmin만 허용

AD 보안 전략

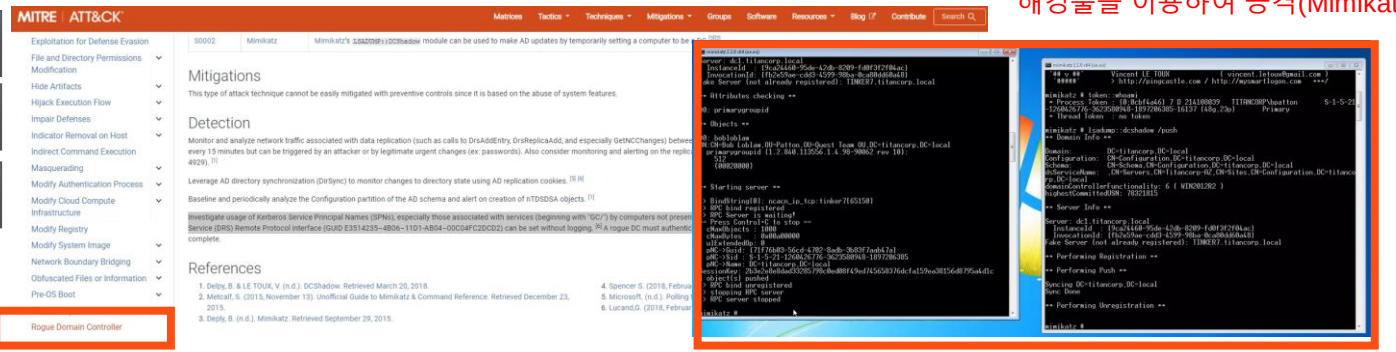
전략 #3 위협탐지

Quest

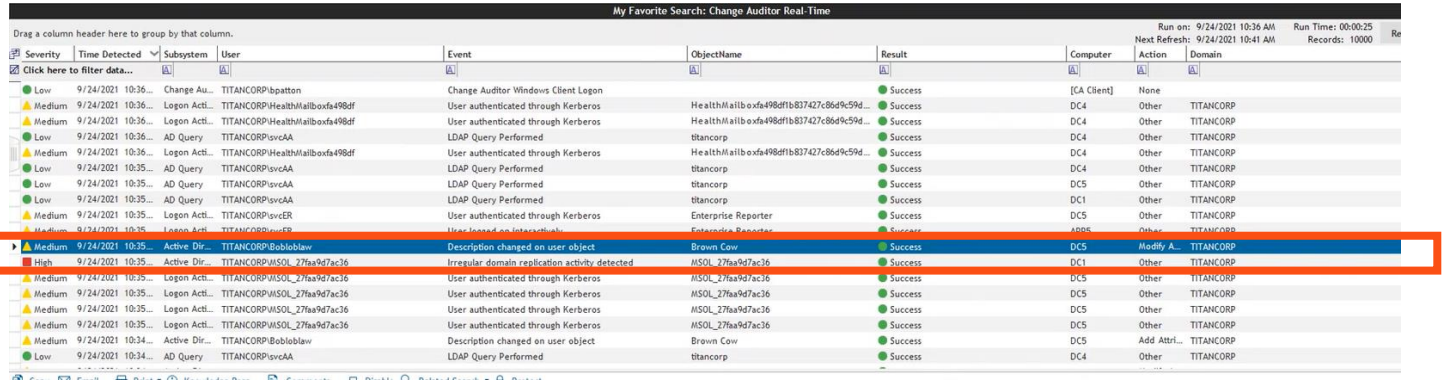
실시간 위협탐지 사례 - DCShadow

- Golden Kerberos Ticket
- SID History Injection
- DC Sync
- DC Shadow
- NTDS.dit
- AdminSDHolder
- Kerberos Roasting

해킹툴을 이용하여 공격(Mimikats)



탐지



AD 보안 전략

전략 #4. 가시성 및 분석체계

Quest

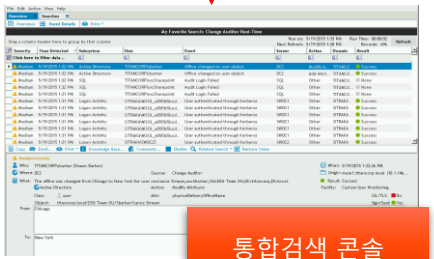
자체 Agent기반의 완벽한 가시성 제공

서버

장기 데이터 저장

SQL Server

장기간 데이터 보관을 하고 이를 전용 Console을 통해서 원하는 조건으로 손쉽게 조회



통합검색 콘솔

Agent설치로 AD에서 발생하는 위협과 변경정보 수집

- 필요한 데이터를 모두 수집
- 적은 서버부하와 데이터 유실 최소화
- 수집된 데이터는 동일 형태의 데이터 제공(누가,무엇을,언제,어디서)

다양한 위협의 탐지나 분석에 최적의 데이터 제공

(**완벽한 가시성 제공**)

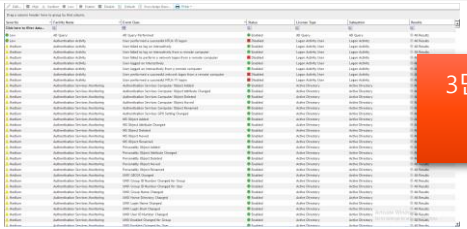
AD 서버

Domain Controller

Domain Controllers

- Active Directory
- Logon Activity

수집 되는 모든 이벤트는 위협도 레벨을 제공

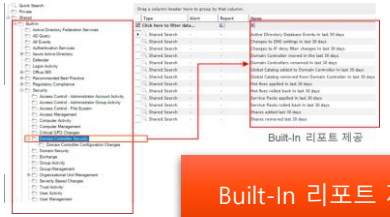


3단계 위협도 정보 제공

High/Medium/Info

Agent를 통해서 자체 데이터를 수집하는 방식을 유일하게 지원

수집된 데이터는 원하는 조건식을 지정하여 별도의 검색 룰로 지정하여 정책위반 감사나 사용자 정의 위협정의 가능



Built-In 리포트 제공

Quest

Where Next Meets Now.

Cyber Resilience

- 통합 인증

Quest

How to Recover From a Ransomware Attack Using Modern Backup

Readily respond to cyberattacks and reduce recovery time

Expert: Fintan Quinn

Ransomware attacks against corporate data centers and cloud infrastructure are growing in complexity and sophistication, and are challenging the readiness of data protection teams to recover from an attack.

Modern backup infrastructure is not a ransomware prevention solution; instead, it is the last line of defense in an overall cybersecurity strategy.

Organizations need to rethink traditional backup infrastructure and invest in technology that provides the best chance of both protecting corporate data and recovering from devastating cyberevents.

This research provides guidance to IT leaders on the recovery of data and services in the aftermath of a ransomware attack by introducing our four-step Ransomware Recovery Guidance Framework.

Complete the form to get your free copy.

Gartner

Gartner

How to Protect Backup Systems From Ransomware Attacks

Published 21 September 2021 - ID G00757692 - 7 min read

By Analyst(s): Nik Simpson

Initiatives: Data Center Infrastructure; Cybersecurity and IT Risk

> Ransomware attacks have grown more frequent and costly over the past year, and have broadened to target backup and other critical infrastructure. This research describes steps that I&O leaders must take to protect backup data from ransomware attacks to facilitate recovery.

Quest

Where Next Meets Now.

대표적인 랜섬웨어 공격

Maersk

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

Molson Coors

의심되는 공격에 **"양조장 운영, 생산 및 배송이 지연되거나 중단"**

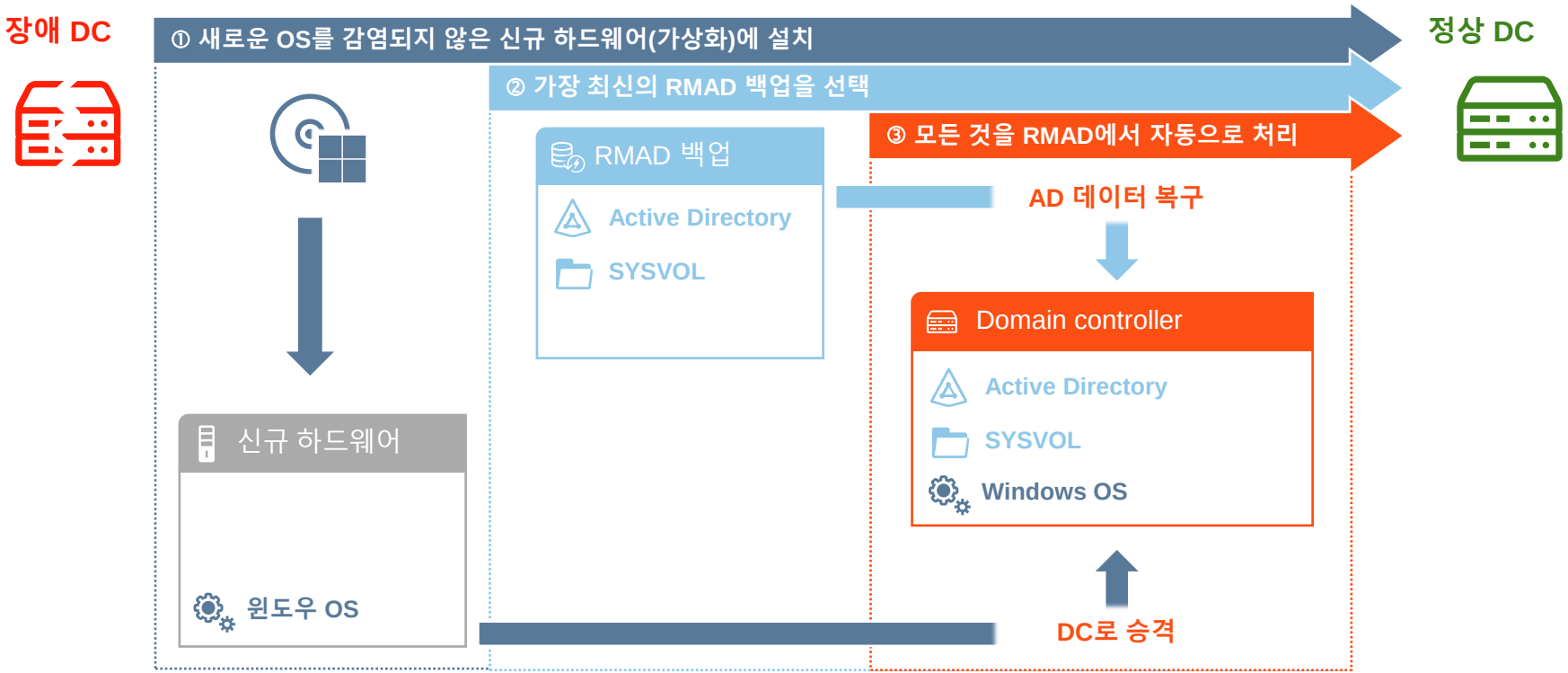
DR 개념의 복구 요건

복구 형태

랜섬웨어 공격에서는 시점 파악이 어렵고

많은 시간이 소비되는 매뉴얼 프로세스 필요

Clean OS 복구


장애 DC
① 새로운 OS를 감염되지 않은 신규 하드웨어(가상화)에 설치
정상 DC
② 가장 최신의 RMAD 백업을 선택
③ 모든 것을 RMAD에서 자동으로 처리
RMAD 백업
Active Directory
SYSVOL
AD 데이터 복구
Domain controller
Active Directory
SYSVOL
Windows OS
신규 하드웨어
윈도우 OS
DC로 승격

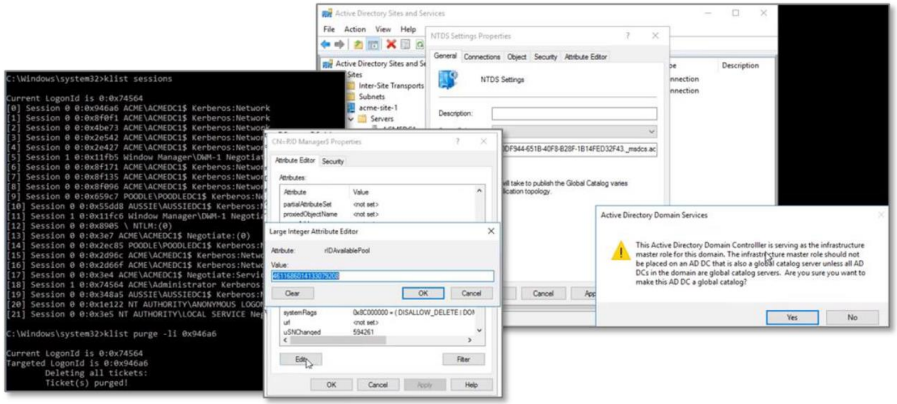
비즈니스 연속성을 위한 복구 시간

자동화된 복구 지원

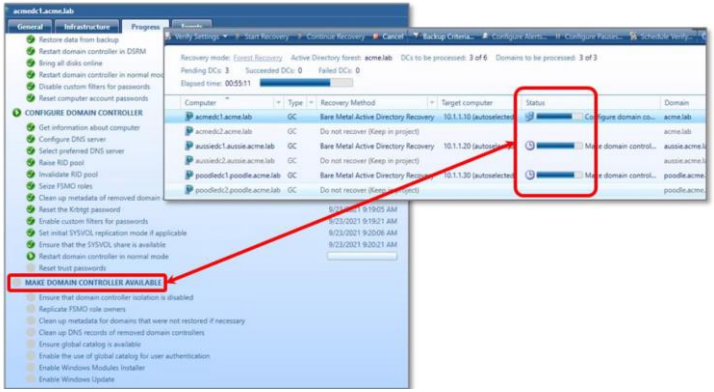
Manual

The process for the third step includes:[8]

1. Verify network connectivity and DNS.
2. Reset the DC computer account passwords.
3. Raise the RID pool, invalidating any published RIDs.
4. Seize FSMO roles for the root domain.
5. Seize FSMO roles for all other domains.
6. Clean up the metadata of other DCs.
7. Reset the KRBTGT account password.
8. Reset internal Trust passwords.
9. Validate SYSVOL share is available.
10. Add the Global Catalog.



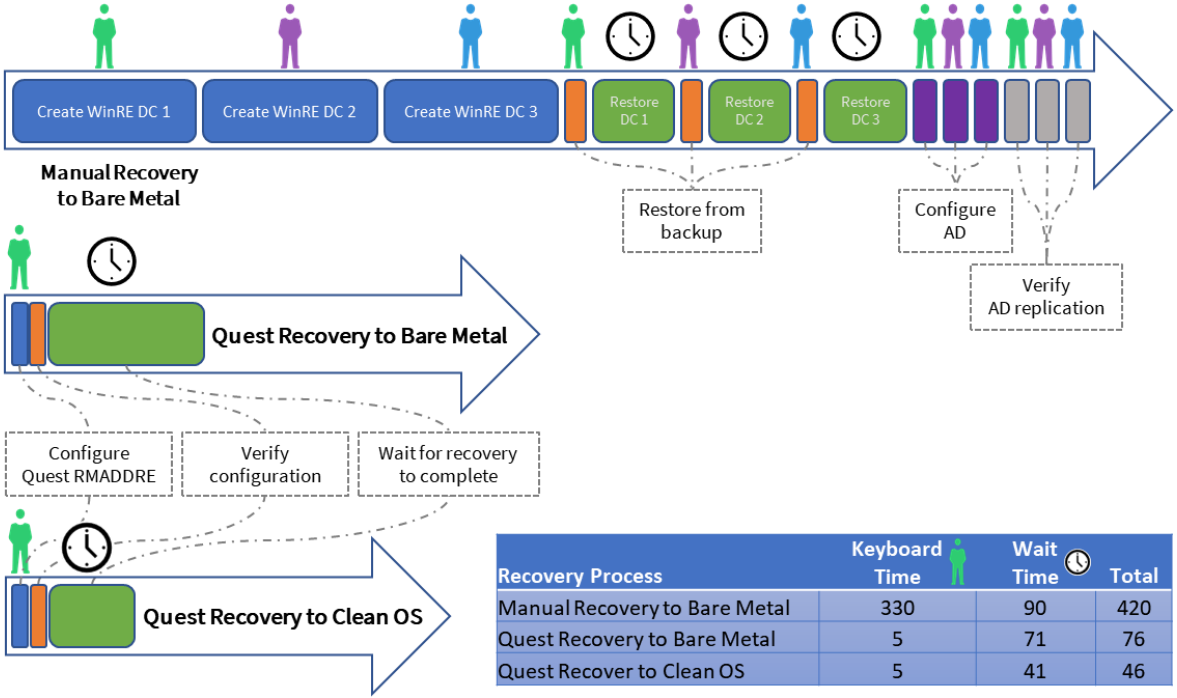
Automation



Quest

Where Next Meets Now.

복구 시간 비교



Recovery Process	Keyboard Time	Wait Time	Total
Manual Recovery to Bare Metal	330	90	420
Quest Recovery to Bare Metal	5	71	76
Quest Recover to Clean OS	5	41	46

Quest는 ?

Quest

Where Next Meets Now.

Microsoft Platform Solutions Leader

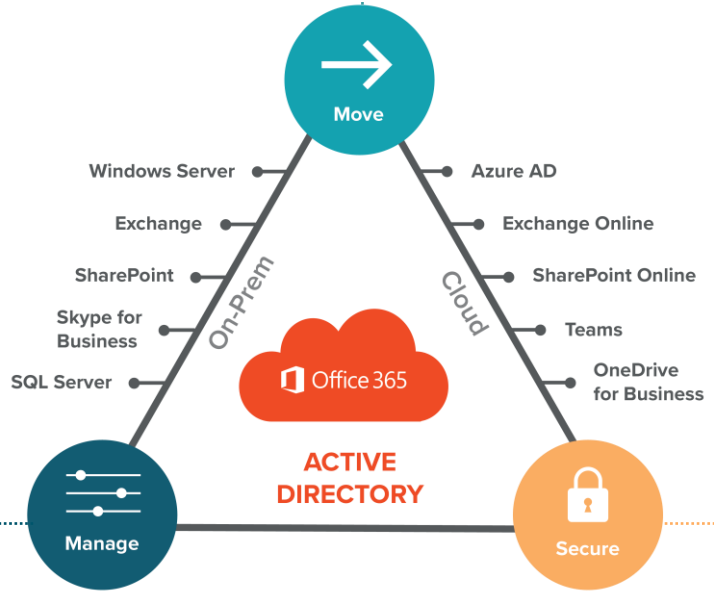
Migrate From:
- Exchange
- PSTs/Archives
- Lotus Notes
- Office 365
- Active Directory
- Windows Server
- Gmail/G Drive
- SharePoint
- OneDrive
- File shares
- Box/Dropbox
- Teams

→ 마이그레이션

Migrate To:
- Office 365
- Active Directory
- Exchange
- SharePoint
- OneDrive for Business
- Teams

관리

- 백업 및 복구
- 리포팅(가시성)
- GPO 관리
- Office 365 라이선스 관리
- AD DR



보안

- 보안위협 보호 와 탐지
- Office 365 최소권한 관리
- 위협 원인 분석
- 보안 감사

Quest

Where Next Meets Now.

Quest의 Hybrid AD cyber resilience

Identify

SpecterOps BHE / Enterprise Reporter Suite / Quadrotech Nova

Protect

Change Auditor / GPOADmin / Quadrotech Nova

Detect

Change Auditor / On Demand Audit Hybrid Suite

Respond

Change Auditor / IT Security Search / Enterprise Reporter Suite

Recover

Recovery Manager DRE / On Demand Recovery

Quest

Where Next Meets Now.


Thank You
Quest
Where Next Meets Now.