

# AD를 통한 랜섬웨어 공격의 모든 것!

Solution Consultant / Hongso Chae

[hongso.chae@quest.com](mailto:hongso.chae@quest.com)

**Quest**

Where Next Meets Now.

# Cybersecurity and Cyber Resilience



Cybersecurity

Reacting

위협에 대한 대응



Cyber Resilience

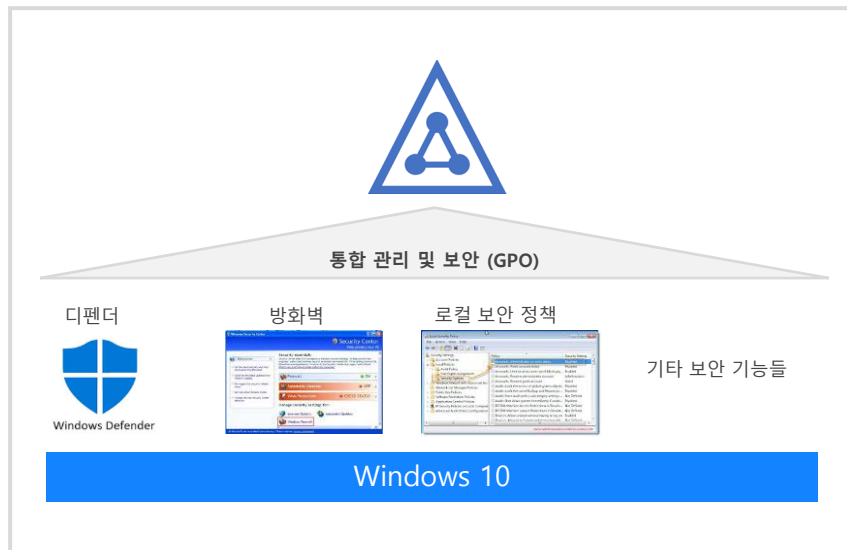
Anticipating

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



대부분의 VDI에서 AD를 통합인증으로 사용



# Cybersecurity

- 단말통합관리



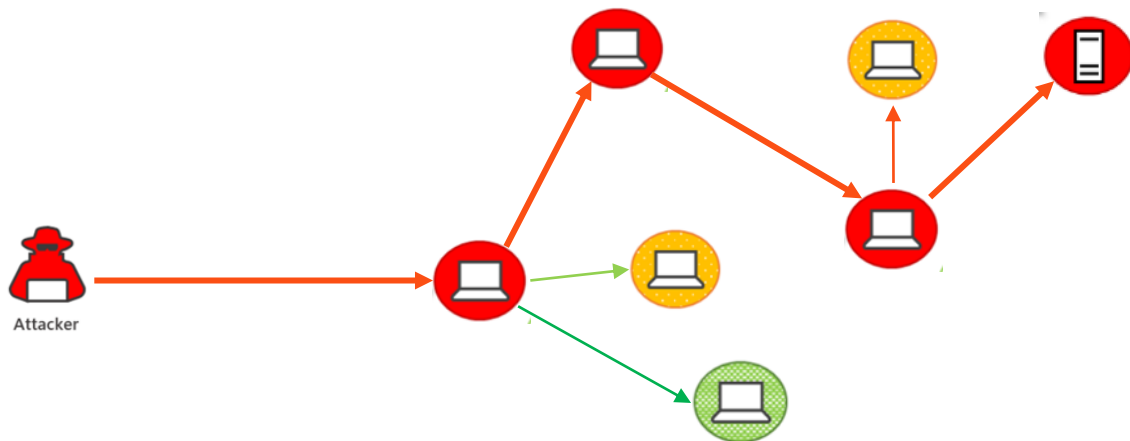
# 단말 보안?

# 단말 보안의 2가지 영역

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

공격보호

내부전파 차단 및 탐지



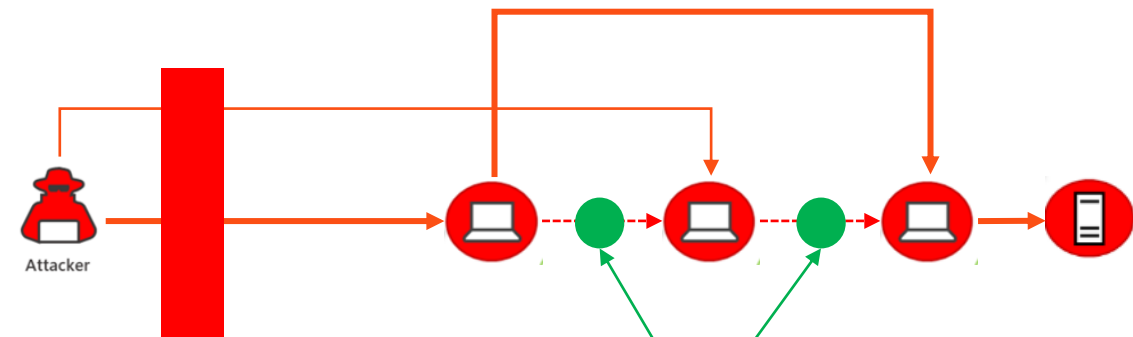


# AD가 없는 환경에서의 단말 보안?

# AD가 없는 환경은 단말보호 솔루션으로..

단말간 위협전파 탐지도

단말 보안 솔루션으로



공격으로부터의 단말 보호는

주로 단말 보안 솔루션

단말간 위협전파 차단은

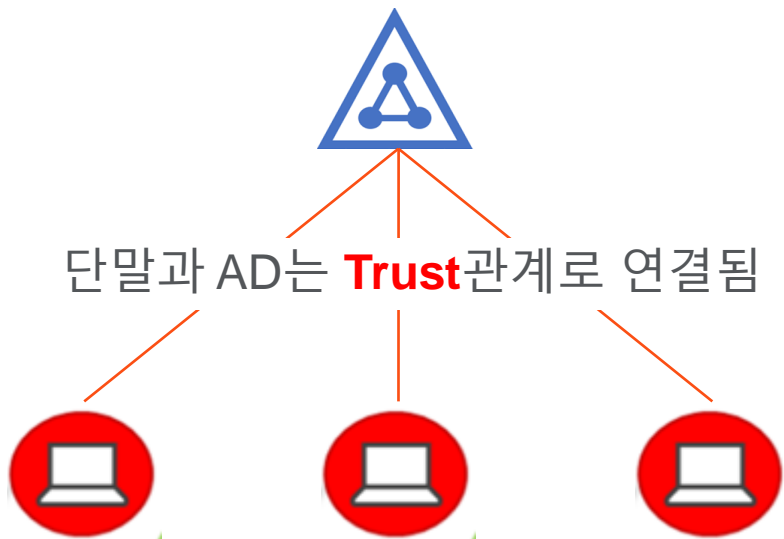
설정을 통한 단말간 연결(RDP, SMB 등) 차단

단말보호 관점의 단말 보안 솔루션과

설정으로 단말 보안

# AD가 있는 환경에서의 단말 보안은?

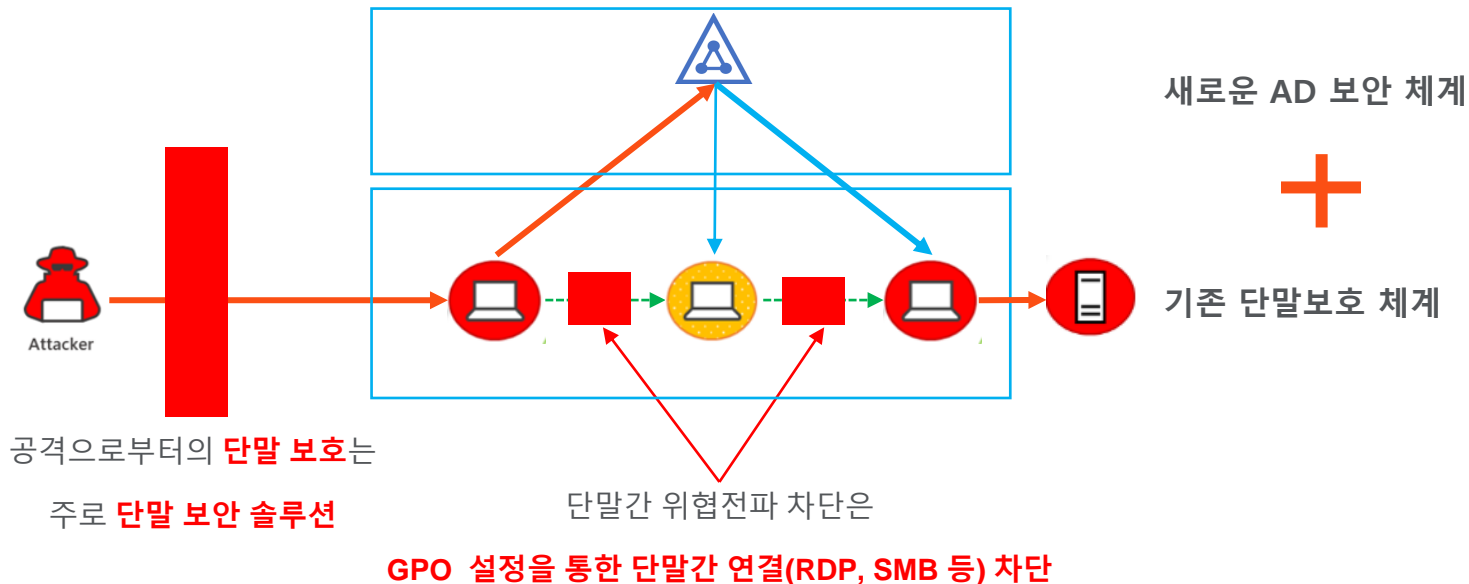
# 단말이 AD로 구성되어 있다는 것은?



# AD 단말 환경에서의 단말보안

단말간 위협전파 차단과 탐지는

AD 보안을 통해서



# 그런데 왜 AD를 통해서 내부 전파?



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



이유 #2. 단말을 개별로 공격하는 것은 **많은 비용** 필요

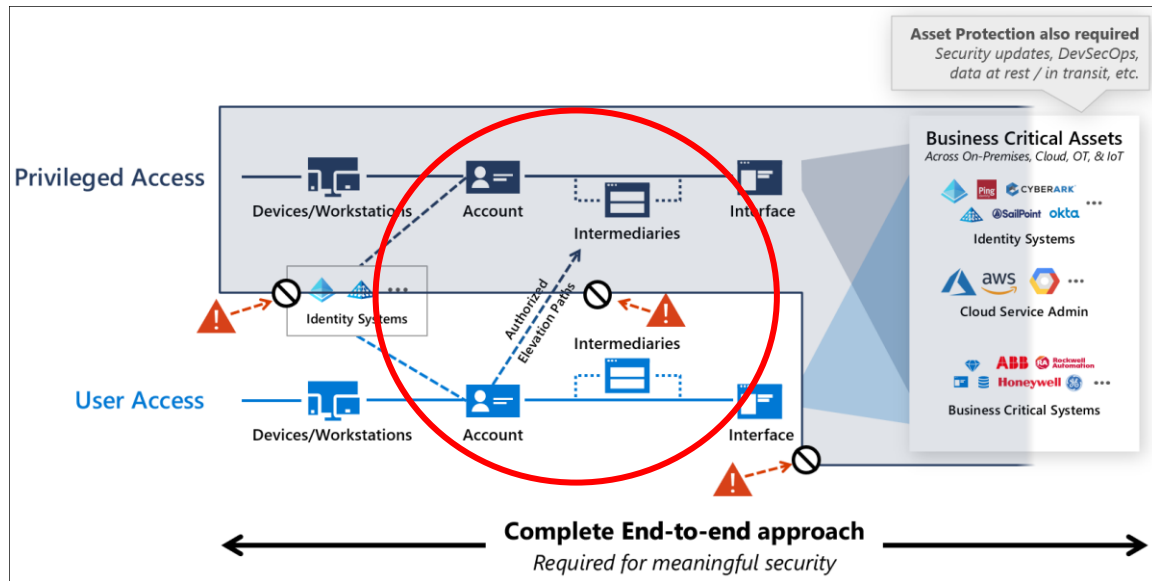
- 직접 연결을 사전에 차단 : 단말간 RDP, SMB 차단
- 공격대상이 너무 많은 : 모든 단말을 개별로 공격

# AD의 위협은?

# 일반 단말을 통한 공격

## Microsoft의 Privileged Access Strategy

공격으로 탈취된 단말  
(대부분 일반 단말)을 통해서 접근

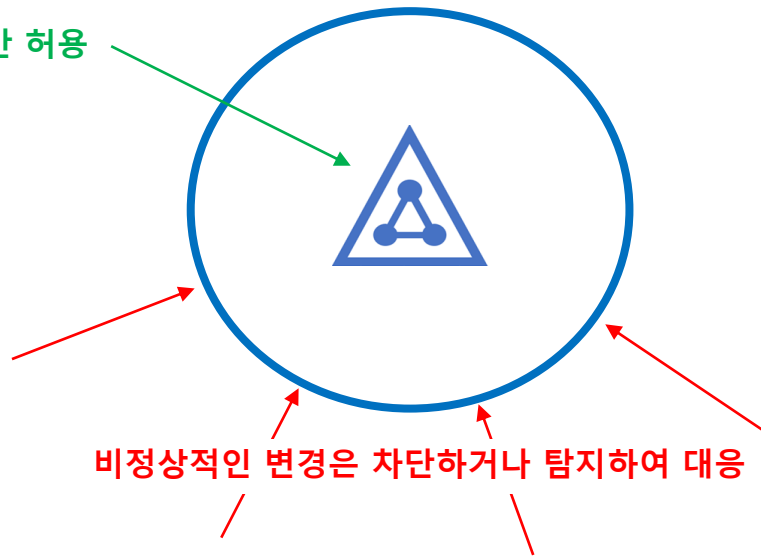




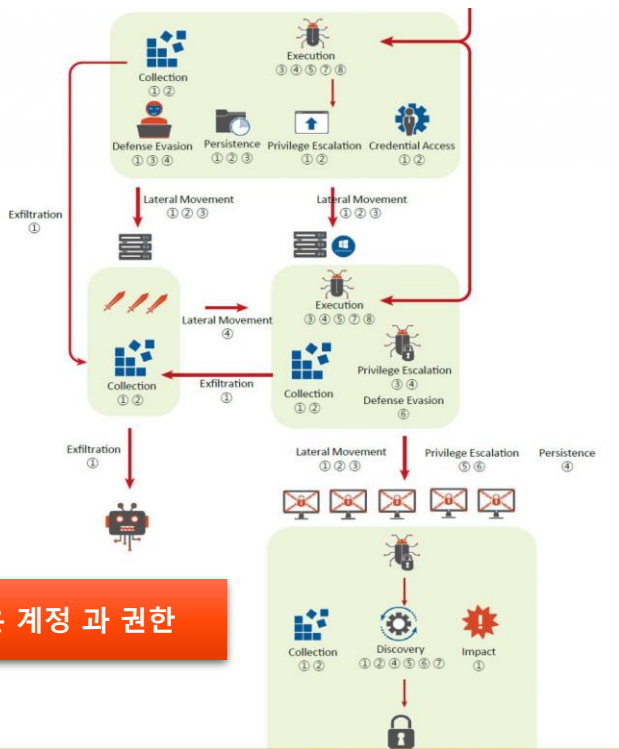
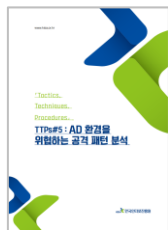
# 높은 권한 계정(권한) 탈취

권한 획득을 위해서는 AD의  
데이터 변경 발생  
(또는 어딘가에 저장된 데이터를  
획득)

정상적인 변경만 허용



# 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 전자 시스템을 점검해보아야한다.

# AD 보안 전략

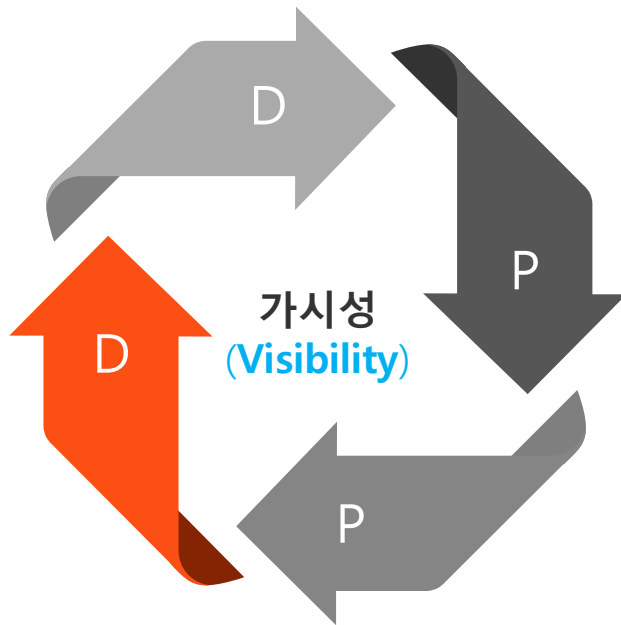
# AD 보안전략(2P2D)

## Diagnostic(분석)

운영과정에서의 분석 및 위협발생에 대한 원인분석을 위한 데이터 및 검색 체계

## Detect(탐지)

AD에 알려진 위협 등을 통한 공격을 실시간으로 탐지하여 피해를 최소화



## Protect(보호)

위협이 될 수 있는 요소를 보호하여 위협요소 사전 차단

## Prevent(예방)

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

# AD 보안 전략

## 전략 #1. 예방

Quest

quest.com | confidential

Where Next Meets Now.

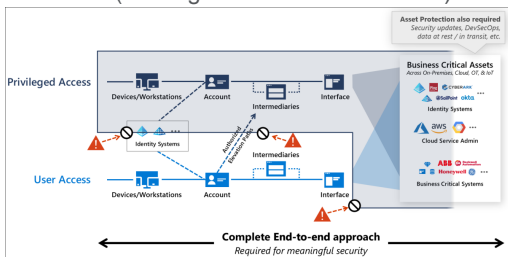


# 정책기반위협을 통한 예방

## 정책 기반 위협

	Enterprise Security	Specialized Security	Privileged Security
	Baseline security for assets + starting point for higher security	Enhanced security profile for higher value assets	Strongest security for highest impact assets and accounts
<b>Account</b> with access to resources	Enterprise Account	Specialized Account	Privileged Account
<b>Profile Summary</b>	<ul style="list-style-type: none"> <li>Enforce Strong MFA</li> <li>Enforce Account/Session risk</li> </ul>	<ul style="list-style-type: none"> <li>Enforce Security Plan...</li> <li>Enforce accounts as sensitive</li> <li>Prioritize security response for accounts</li> </ul>	<ul style="list-style-type: none"> <li>Specialized Security Plan...</li> <li>Enforce restrict account usage to specific devices</li> <li>Enforce monitor for anomalous usage within the enterprise</li> </ul>
<b>Security Benefit</b> Monitor risk reduction across your network from user activity	<ul style="list-style-type: none"> <li>Insider Coercion/Estortion</li> <li>Targeted Workstation Compromise</li> </ul>	<ul style="list-style-type: none"> <li>Insider Coercion/Estortion</li> </ul>	<ul style="list-style-type: none"> <li>Insider Coercion/Estortion with sophisticated execution</li> </ul>
<b>Implementation Effort/Cost</b>	<ul style="list-style-type: none"> <li>Configure strong MFA &amp; educate users</li> <li>Require account/session risk in conditional access policy</li> <li>Integrate alerts into Security Operations / SOC processes</li> </ul>	<ul style="list-style-type: none"> <li>Enterprise Security Plan...</li> <li>Update security operations / policies</li> <li>Educate security operations personnel (analysts, threat hunters, incident manager, etc.)</li> </ul>	<ul style="list-style-type: none"> <li>Specialized Security Plan...</li> <li>Determine authorized devices and patterns for role</li> <li>Design restrictions and monitoring for each role</li> <li>Update security operations processes and educate personnel</li> </ul>

## PAW(Privileged Access Workstation)



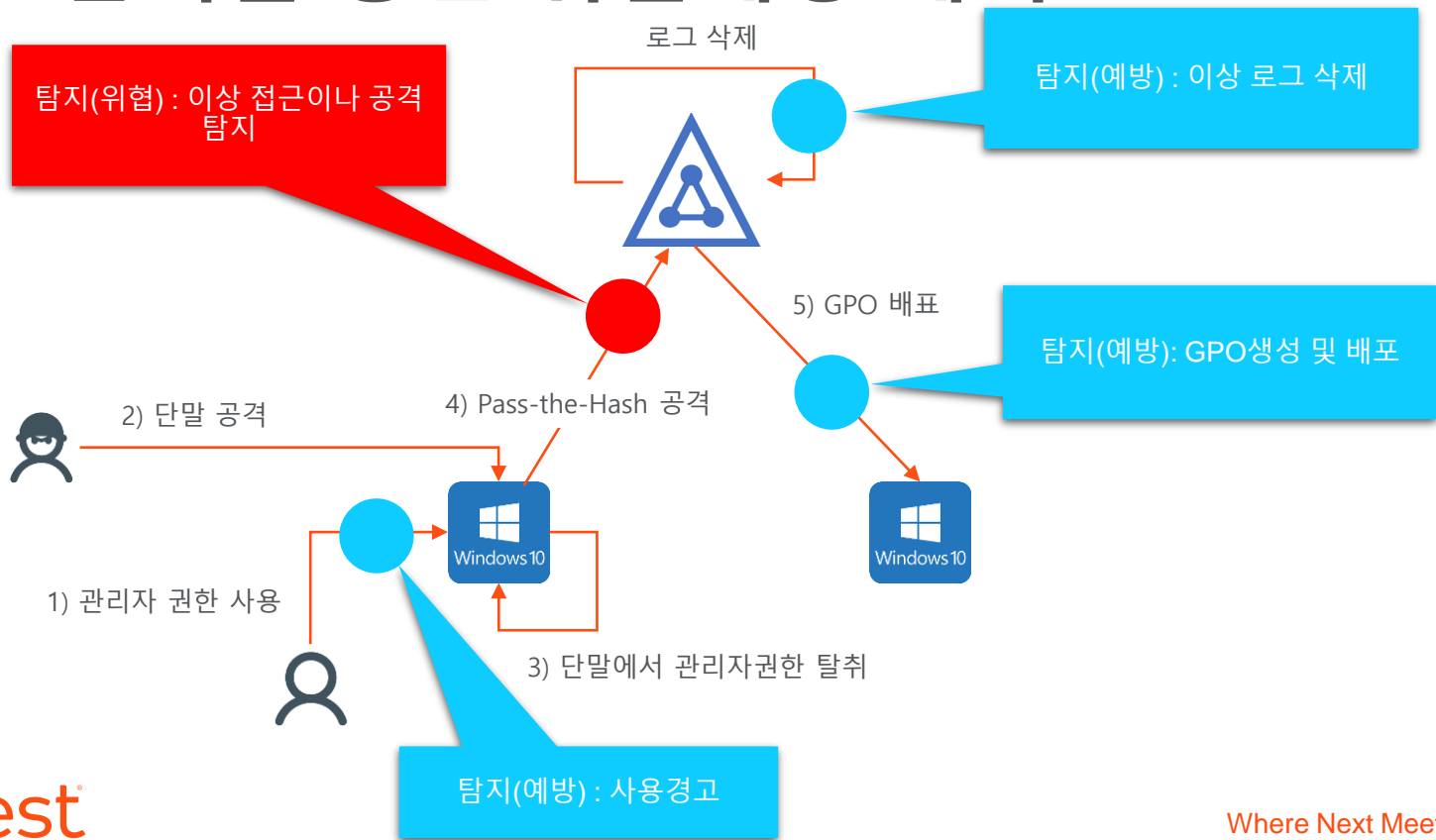
## Privileged Access Strategy

## 공통적인 위협

- 일반 단말에서 관리자 계정 사용
  - 방화벽정책 비활성화
  - 기본 Administrator 계정 활성화
  - Guest계정 활성화
  - 허용되지 않은 경로에서의 사용자 계정 추가
- 
- 계정 별 허용되지 않은 작업 수행
  - 허용되지 않은 위치에서의 접근(관리자권한 계정)
  - 퇴직자 계정 활성화

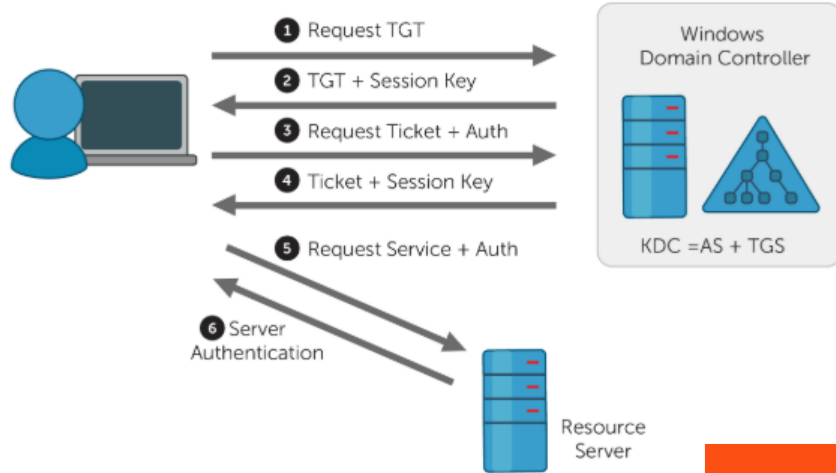
## 회사내부 보안정책기반 위협

# 사전 탐지를 통한 위협예방 예시



# 사전 탐지를 통한 위협예방 사례

## Kerberos Roasting 공격 : Kerberos를 통해서 계정탈취



```

This means that hashtcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashtcat.net/faq/morework

Approaching final keyspace - workload adjusted.

$krb5tgs$23428bdc5e4e514a94b561156069953e0c85e4ddac618c74978d7b0b2416b17884808f820ae5856e07d654a234d72c74c163f1df4c3f1845
b15e2de199f745ddf9ac8a118224c17439fc0f8bb1c82bc8c818418e370fab8722173ca7088791a832c36bc5e8bd23e25a9cfc7b7be728399e83
179f0eb0c9f9a11c0261c73d34c2bae76185a9abd9e9b18cfe90ad29c139a3aad9573187f716c64109594c1a13f3c7c808e79765d7794b747f
14d52f6e594e13129869a956626fca37c52a9fab880c32c4d5ebaf1fa5208410bf18e59f705708becfa09100315393f7171084bcfd99a
0313f7b2f83fae337200edca322073525c9af8aeb9813f95e0d953226bc1dd05e02836a80102212b7d9cf4270797080bf0be288ba7f5b3844a
5427bdf173288868db9a9b6afe667596bb198b609d52f809786f1805905c88478f1aa8c04b0d8421d89ce9d515a5bab74131273c2635c3cb352
81cf9afd69cfffca7be73bee74aa7462e53de897cdca120b67977a64dffcc5db4514a8c4924146b2b436a5e70b70d59e4b3fc8929878a35c2e8991
ea9c33dc92c04f8c7e4c8e2a03fe0bf880f7d89cea1d2a299b5eab9227ec01dd410cfecc4e6613615058c2a0972c3adfec5b25f9fadb14365b
0850463adfb543957c670809014450323fcf836e7f31100909fc186a101463a1698cf0fa6307fca2beded10711c1aad10b76610c206170e0ccbc
50ca2307fa620cb95d32486529bf570e47bd652b078a258f6da7b6cfe291f763eef1394d39f58e38f201ee34080bdad6e5508252369db2c6671b
ff700474b18299db9fc6896f272e9882daeda312347fe04d337283859fedf2bbdb5dba164696596cc527278313e607853e849af896e6936c70739
16d635af6de3a224d727a9a92379397fe166f6e3d33c3dbfae7b23f5dcafa284948ae3d925edcc51e163aeca84838bd09924c02217068296092ca7f24
e0804e71169b734519eed89bd8edf445af38b3a3407a2350f1bad8de558553ce87d64b1d7adffc6f978ae8fa39b8e2835484028816c4ddff9a6d313
900121c95e90fe2fe3b3538f7f7eb537ce1d5f69f9065b3fe938f65f76e9542391f6586b25a01bc5da9678daaca690b5a79c0065c4411940caeece
3e44f09e47c5742957270d70b4920511389e2e0b490b3607ab0c4d5e995228cb16190751754dc55399c85a8c4e9e8019972a91d4f21df60b
77d3e1cfb70f113635936c15e38f217ee4152e11864d0e6e7fa222018c11d61b569f3c80e5af736ed3a308518fa688594190e9680273db69c00fe
602e3d773ce8d407bf420f78bb40b3225b409eae791b44ee77f707576d638e4796cfe73432c50729232732928fdad0646492924737b1891e3da3e
9fb2c63aa085ad297bf8df7ced200dfb7a7662770172eeacc220c06f882bdc1edc3b963e84db4a706147476921269992d38aad570e416a352e85d6
f370861fadf3205c3d3931c76242c6bbe17c2003cddb410097269534d51475c98add3c14162b848d4e6cdfb1586db290243000620595d0e0095b6
68efa8026e824abfc743f061c20f768726f68f50614563a1b7614846a467c4757ce403554b306863e639e38d7640088Pa$word1234
    
```

국내 고객사에서 일부단말에서 해당 공격을 위해서 필요한 ServicePrincipalName의 비정상 변경을 확인하여 해당 공격 사전 대응



Where Next Meets Now.



# AD 보안 전략

## 전략 #2. 보호



# 알려진 위협이나 회사 보안정책 위반 보호

변경 되었을 때 영향도가 큰 변경 보호

전사 보안 GPO( Default GPO )

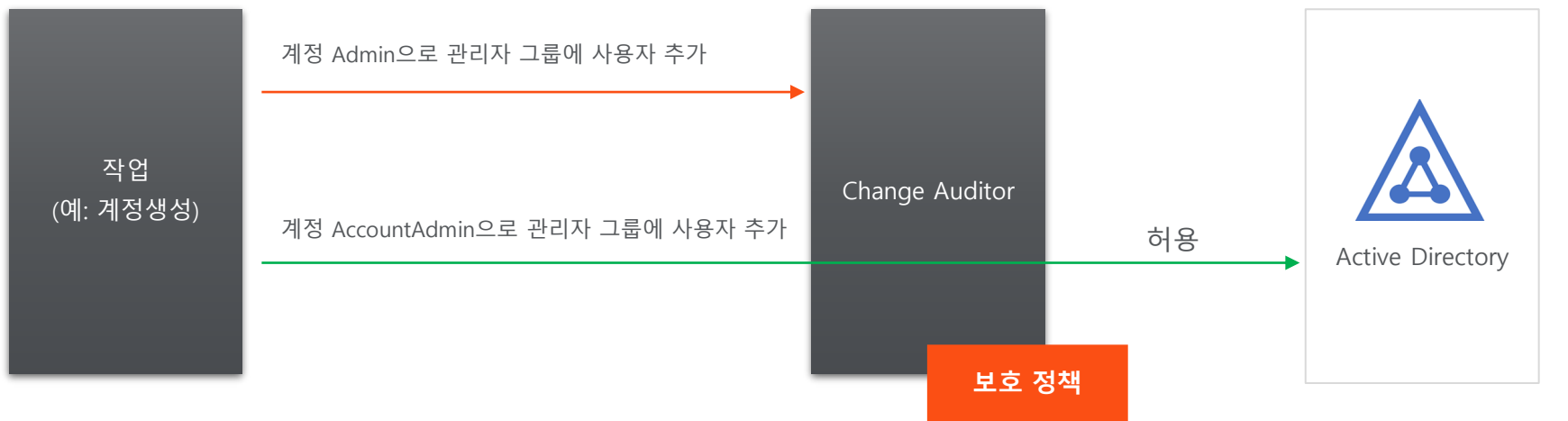
최상위 관리자만 작업을 할 수 있거나  
변경이 되었을 때 큰 보안위협이 될 수 있는 항목

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

quest.com | confidential

Where Next Meets Now.



# 실시간 위협탐지 사례 - DCSshadow

해킹툴을 이용하여 공격(Mimikats)

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

**MITRE ATT&CK**

Exploitation for Defense Evasion

File and Directory Permissions Modification

Hide Artifacts

Hijack Execution Flow

Impair Defenses

Indicator Removal on Host

Indirect Command Execution

Masquerading

Modify Authentication Process

Modify Cloud Compute Infrastructure

Modify Registry

Modify System Image

Network Boundary Bridging

Obfuscated Files or Information

Pre-OS Boot

**Rogue Domain Controller**

**Mitigations**

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

**Detection**

Monitor and analyze network traffic associated with data replication (such as calls to DrsAddentry, DrReplicatAdd, and especially GetNCCChanges) between every 15 minutes but can be triggered by an attacker or by legitimate urgent changes (ex. passwords). Also consider monitoring and alerting on the registry 4929. <sup>[1]</sup>

Leverage AD directory synchronization (DirSync) to monitor changes to directory state using AD replication cookies. <sup>[2]</sup>

Baseline and periodically analyze the Configuration partition of the AD schema and alert on creation of sTDSOA objects. <sup>[3]</sup>

Intelligent usage of Kerberos Service Principal Names (SPNs), especially those associated with services (beginning with "SP") by computers not present in Service (SRV) Remote Protocol Interface (GUID E3514235-4805-1101-A054-000AF4C20C22) can be set without logging. <sup>[4]</sup> A rogue DC must authenticate completely.

**References**

1. Depp, B. & E. TOUL, V. (n.d.). DCSshadow. Retrieved March 20, 2018.
2. Miskat, S. (2018, November 13). Unofficial Guide to Mimikatz & Command Reference. Retrieved December 23, 2015.
3. Depp, B. (n.d.). Mimikatz. Retrieved September 29, 2015.
4. Spencer S. (2018, February 2015). Microsoft. (n.d.). Auditing. & Luciani, G. (2016, February 2015).

```

mimikatz & [Admin: admin]
Process: lsass - (E 9345461 7 B 214180809 ITINCRP\SvcAuth
15026776-9C258048-189786305-16137 148y.3k) Primary
Terminal Name: no icon

mimikatz & [Admin: dcsshadow /usb
-- Domain Info --
Domain: DC11titancorp.local
Configuration: DC-Configuration,DC11titancorp.local
Schema: DC-Schema,DC-Configuration,DC11titancorp.local
Logon: DC-Logon,DC-Servers,DC11titancorp.local
Authentication: DC-Authentication,DC11titancorp.local
Status: (0x00000000) 00201515
-- Server Info --
Server: DC11titancorp.local
InstanceID: [64b68c56-478a-c209-f48f37f84ac]
[localization] [15026776-9C258048-189786305-16137]
Fake Server (not already registered): [189B7711titancorp.local]
Authentication: [00201515]
-- Performing Push --
Syncing DC11titancorp.local
-- Performing Unregistration --
mimikatz &
    
```

탐지

My Favorite Search: Change Auditor Real-Time

Run on: 9/24/2021 10:36 AM Run Time: 00:00:25

Severity	Time Detected	Subsystem	User	Event	ObjectName	Result	Computer	Action	Next Refresh	Records
Low	9/24/2021 10:36...	Change Au...	TITANCORP\bpattan	Change Auditor Windows Client Logon		Success	[CA Client]	None	9/24/2021 10:41 AM	10000
Medium	9/24/2021 10:36...	Logon Act...	TITANCORP\HealthMailboxfa498df	User authenticated through Kerberos	HealthMailboxfa498df18517427-86d9c59d...	Success	DC4	Other	TITANCORP	
Low	9/24/2021 10:36...	AD Query	TITANCORP\svca	LDAP Query Performed	titancorp	Success	DC4	Other	TITANCORP	
Medium	9/24/2021 10:36...	Logon Act...	TITANCORP\HealthMailboxfa498df	User authenticated through Kerberos	HealthMailboxfa498df18517427-86d9c59d...	Success	DC4	Other	TITANCORP	
Low	9/24/2021 10:35...	AD Query	TITANCORP\svca	LDAP Query Performed	titancorp	Success	DC4	Other	TITANCORP	
Low	9/24/2021 10:35...	AD Query	TITANCORP\svca	LDAP Query Performed	titancorp	Success	DC5	Other	TITANCORP	
Low	9/24/2021 10:35...	AD Query	TITANCORP\svca	LDAP Query Performed	titancorp	Success	DC1	Other	TITANCORP	
Medium	9/24/2021 10:35...	Logon Act...	TITANCORP\svcer	User authenticated through Kerberos	Enterprise Reporter	Success	DC5	Other	TITANCORP	
Medium	9/24/2021 10:35...	Logon Act...	TITANCORP\svcer	User authenticated through Kerberos	Enterprise Reporter	Success	DC5	Other	TITANCORP	
Medium	9/24/2021 10:35...	Active Dir...	TITANCORP\Bobloblaw	Description changed on user object	Brown Cow	Success	DC5	Modify A...	TITANCORP	
High	9/24/2021 10:35...	Active Dir...	TITANCORP\WISOL_27fa9d7ac36	Irregular domain replication activity detected	WISOL_27fa9d7ac36	Success	DC1	Other	TITANCORP	
Medium	9/24/2021 10:35...	Logon Act...	TITANCORP\WISOL_27fa9d7ac36	User authenticated through Kerberos	WISOL_27fa9d7ac36	Success	DC5	Other	TITANCORP	
Medium	9/24/2021 10:35...	Logon Act...	TITANCORP\WISOL_27fa9d7ac36	User authenticated through Kerberos	WISOL_27fa9d7ac36	Success	DC5	Other	TITANCORP	
Medium	9/24/2021 10:35...	Logon Act...	TITANCORP\WISOL_27fa9d7ac36	User authenticated through Kerberos	WISOL_27fa9d7ac36	Success	DC5	Other	TITANCORP	
Medium	9/24/2021 10:35...	Logon Act...	TITANCORP\WISOL_27fa9d7ac36	User authenticated through Kerberos	WISOL_27fa9d7ac36	Success	DC5	Other	TITANCORP	
Medium	9/24/2021 10:34...	Active Dir...	TITANCORP\Bobloblaw	Description changed on user object	Brown Cow	Success	DC5	Add Attr...	TITANCORP	
Low	9/24/2021 10:34...	AD Query	TITANCORP\svca	LDAP Query Performed	titancorp	Success	DC4	Other	TITANCORP	



Where Next Meets Now.

# AD 보안 전략

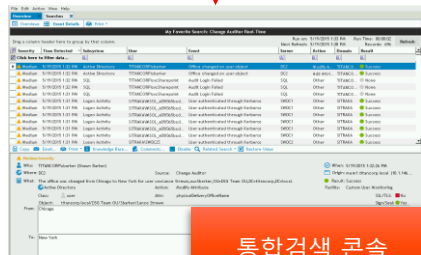
## 전략 #4. 가시성 및 분석체계



# 자체 Agent기반의 완벽한 가시성 제공



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



통합검색 콘솔

서버

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)**

수집 되는 모든 이벤트는 위협도 레벨을 제공

3단계 위협도 정보 제공  
High/Medium/Info

AD 서버

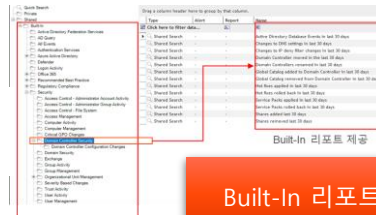
Domain Controller



- Active Directory
- Logon Activity

Agent를 통해서 자체 데이터를 수집하는 방식을 유일하게 지원

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



Built-In 리포트 제공

# Cyber Resilience

- 통합 인증

Quest

quest.com | confidential

Where Next Meets Now.





# 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**

**Quest**

**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.

**“Accelerate recovery from attacks by adding a dedicated tool for backup and recovery of Microsoft Active Directory.” – Gartner**

**See how to automate AD disaster recovery**



Where Next Meets Now.

# 대표적인 랜섬웨어 공격



## Maersk

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



## Molson Coors

의심되는 공격에 “양조장 운영, 생산 및 배송이 지연되거나 중단”

# DR 개념의 복구 요건

# 복구 형태

데이터 복구

OS 복구

Clean OS 복구

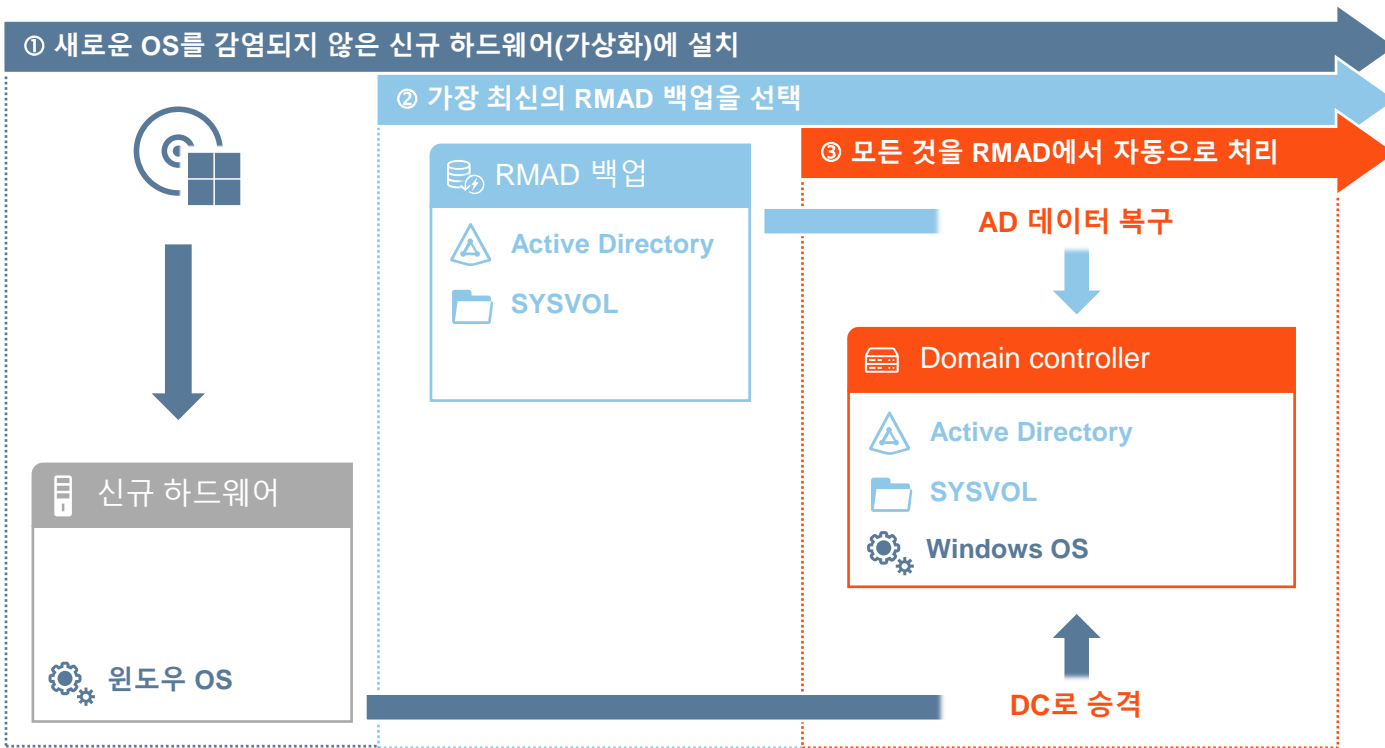
Cloud 복구

---

랜섬웨어 공격에서는 시점 파악이 어렵고  
많은 시간이 소비되는 매뉴얼 프로세스 필요

# Clean OS 복구

장애 DC



정상 DC



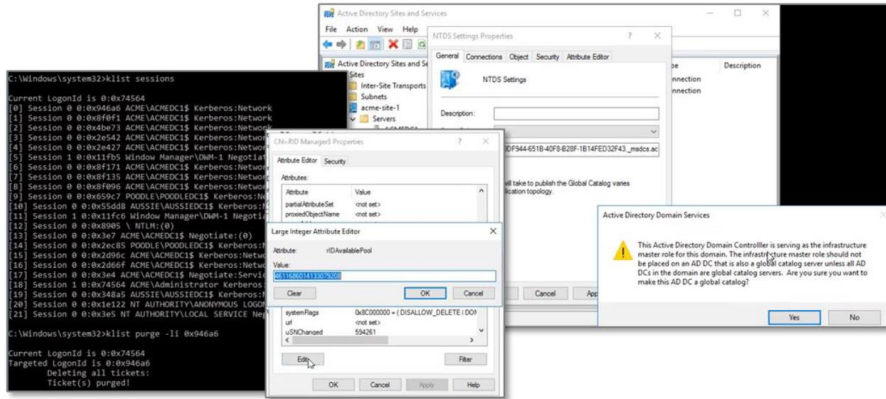
# 비즈니스 연속성을 위한 복구 시간

# 자동화된 복구 지원

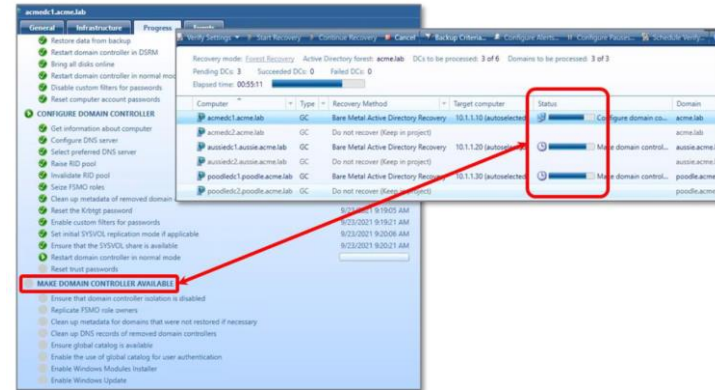
## Manual

The process for the third step includes:<sup>8</sup>

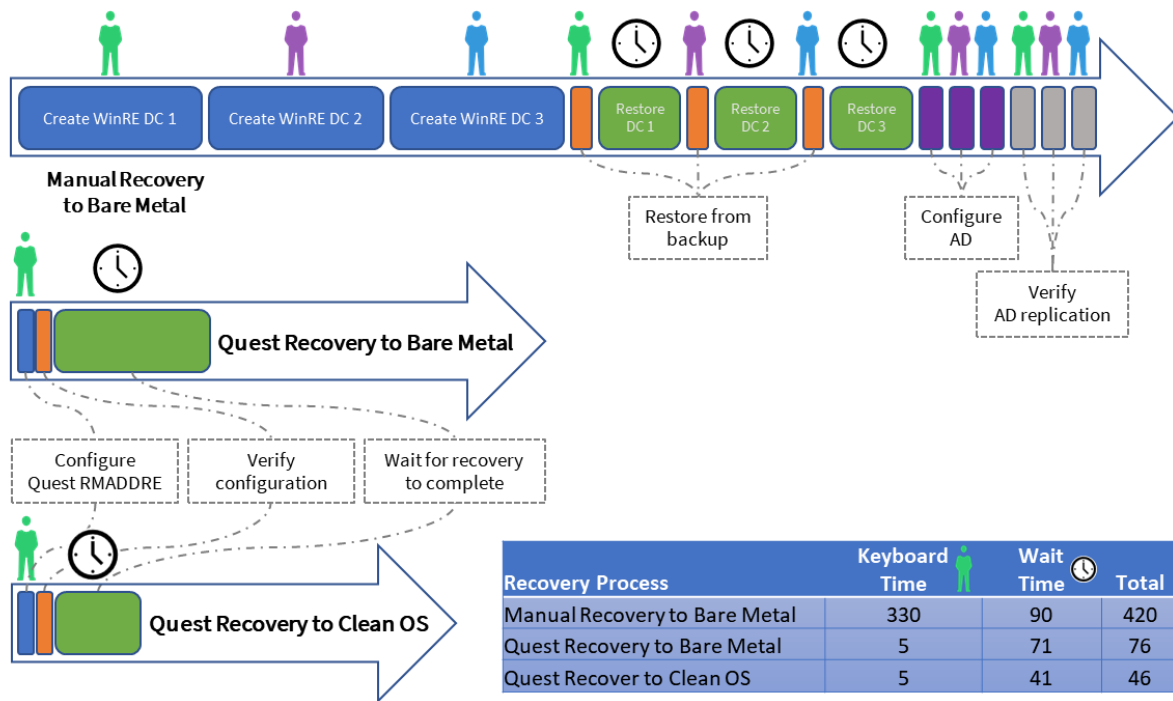
1. Verify network connectivity and DNS.
2. Reset the DC computer account passwords.
3. Raise the RID pool, invalidating any published RIDs.
4. Seize FSMO roles for the root domain.
5. Seize FSMO roles for all other domains.
6. Clean up the metadata of other DCs.
7. Reset the KRBTGT account password.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



## Automation



# 복구 시간 비교





# Quest는 ?

Quest

quest.com | confidential

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

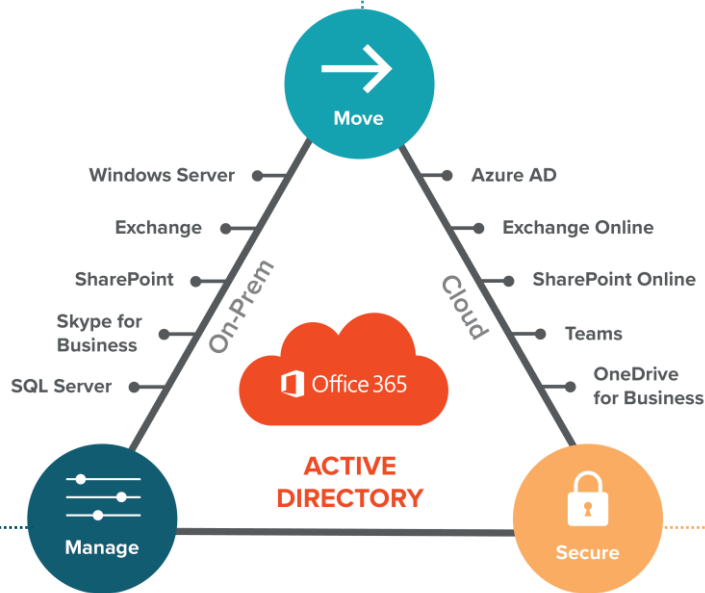
→ 마이그레이션

## 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 보호와 탐지
- Office 365 최소권한 관리
- 위협 원인 분석
- 보안 감사

# 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



Thank You

Quest  
Where Next Meets Now.