

# AD기반 단말 환경에서의 랜섬웨어 예방 및 실시간 탐지 전략

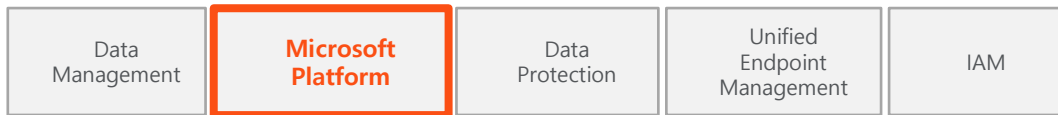
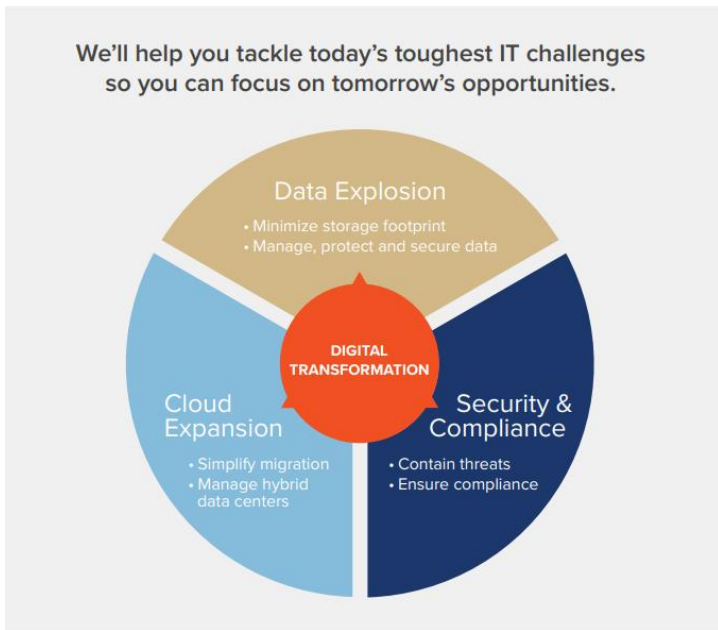
Solution Consultant

Hongso Chae(Hongso.chae@quest.com)

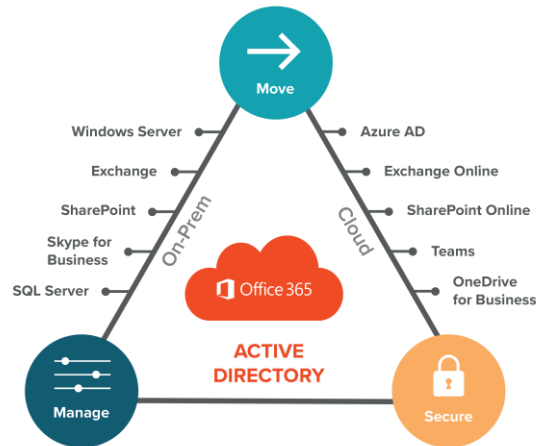
# 회사소개

Quest는 빠르게 변화하는 엔터프라이즈 IT 환경을 위한 소프트웨어 솔루션을 제공합니다.

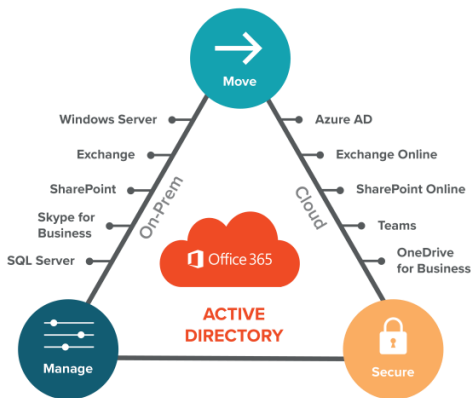
Quest는 데이터 폭발, 클라우드 확장, 하이브리드 데이터 센터, 보안 위협 및 규정 요구사항으로 인한 문제를 단순화할 수 있도록 지원하며 Fortune 500 대 기업의 95%와 Global 1000 대 기업의 90%를 포함하여 100 개국 130,000여 기업에 글로벌 서비스를 제공하고 있습니다.



## 2년 연속 Microsoft 최우수 Global ISV



# Quest Security Solution Overview



AD 보안  
(랜섬웨어 전파 차단 및  
실시간 탐지)

- GPO 접근통제 및 통합관리 : **GPOAdmin**
- AD 계정 접근통제 및 통합관리 : **Active Roles**
- 실시간 위험 탐지 및 감사 : **Change Auditor for AD**, Exchange 등
- 복구 솔루션 : **Recovery Manager for AD**

통합 패스워드 관리

- 통합 시스템, 네트워크, 어플리케이션 패스워드 관리: **One Identity Safeguard Password**

스트리밍 기반의 기록 및  
녹화

- 기록 및 녹화(Citrix VDI, HTTPS 등): **One Identity Safeguard Session**

통합 단말 관리 기반  
패치 및 배포

- 패치 및 배포 관리 : **KACE SMA(System Management Appliance)**

재택근무 보안

- 스트리밍 기반 기록/녹화 전문: **One Identity Safeguard**
- AD기반 Windows 운영체제 2FA : **Defender**
- 패치 및 배포 관리 : **KACE SMA(System Management Appliance)**

# 1. AD보안 필요성





# 랜섬웨어 대응 방식의 변화

# 랜섬웨어 공격의 증가

HOME > 뉴스 > 보안

## “지난해 하반기 랜섬웨어 7배 증가”

김선애 기자 | 승인 2021.03.11 09:11 | 댓글 0

RaaS 진화로 대규모 몸값 요구...의료·전문 서비스 기업·공공·금융 타깃  
솔라윈즈, 전 세계에 피해 입혀...재택근무로 공격 더 쉬워져

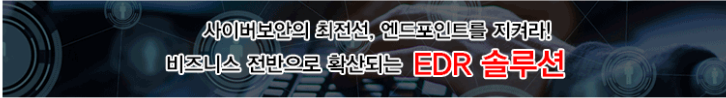
[데이터넷] 지난해 하반기 랜섬웨어 공격이 7배 증가했으며, 올해도 랜섬웨어는 가장 심각한 사이버 위협이 될 것으로 보인다. 포티넷의 '2020년 하반기 글로벌 위협 전망 보고서'에 따르면 지난해 하반기 랜섬웨어가 상반기 보다 7배 증가한 것으로 집계됐다.

# 랜섬웨어 형태의 변화->3중 협박

2021년, 이중 협박의 랜섬웨어는 삼중 협박이 된다

👍 좋아요 7개 | 입력: 2021-02-15 19:54

🔒 📄 🏠 🏠 🌐 🐦 🌐 📺



#정보보호 #경보보안 #IT보안 #사이버보안

범죄자들끼리의 협업과 소통이 원활해지고 있다. 그러면서 서로의 장점들이 퍼지고 개발되고 있다. 코로나와 싸우는 의료 기관에는 안 좋은 소식이다. 게다가 이중 협박 전략은 곧 삼중 협박으로 진화할 예정이라고 하니, 의료 산업을 어이할꼬.

[보안뉴스 문가용 기자] 사이버 범죄 조직들 간 협업과 소통이 갈수록 향상되고 있어 랜섬웨어 공격이 보다 더 위협적으로 변하고 있다고 CTI 리그(CTI League)가 발표했다. 특히 헬스케어 분야를 겨냥한 랜섬웨어 공격이 상당히 위협적으로 진화한 상태라고 한다. CTI 리그는 작년 3월부터 활동을 시작한 전 세계적 자원 봉사 단체로, 의학 분야의 사이버 사건 대응에 특화되어 있다.

CTI 리그는 지난 주 자신들의 활동 내역을 요약한 보고서를 통해 “올해 랜섬웨어 공격은 물론 그와 관련된 활동들(개인 건강 및 식별 정보가 포함된 데이터베이스의 거래 등)이 증가할 것”이라고 예측했다. 또한 지난 한 해 랜섬웨어 공격자들에게 전성기를 가져다 준 ‘이중 협박’ 전략이 ‘삼중 협박’으로 진화할 것이라고 예상하기도 했다. 이들이 말하는 삼중 협박 전략이란 데이터 탈취와 데이터 암호화에 디도스 공격을 더하는 것을 말한다. 의료 산업의 피해자들이 돈을 낼 수밖에 없도록 더 목을 죄겠다는 것이다.

## 삼중 협박



백업복구와 같은 데이터 암호화를 대응하는 랜섬웨어 대책도 중요하지만  
**예방하고 탐지하는 영역의 중요성이 증대**

# 랜섬웨어 형태의 변화->Supply Attack

미국 CISA, “솔라윈즈 공격자들, 정말로 SAML 토큰에 접근했다”

2021-01-08 20:27



가 + 가 -



솔라윈즈 공격자들이 SAML 인증 토큰에 접근했다는 의혹은 이전부터도 있어 왔다. 그런데 CISA가 오늘 “진짜 그랬다”고 고개를 끄덕였다. SAML 인증 토큰이 외부인에게 노출되었다는 건 네트워크를 전체적으로 재구축할 정도의 큰일이라는 말과 함께.

[보안뉴스 문가용 기자] 미국 국토안보부 산하 사이버 보안 전담 조직인 CISA가 솔라윈즈(SolarWinds) 사태와 관련하여 새로운 소식을 전했다. 공격자들이 실제로 SAML 인증 토큰을 남용했음을 나타내는 새로운 증거를 찾아냈다는 것이다. 공격자가 SAML 인증 토큰에 접근하는 데 성공할 경우 인증 과정이 완전히 망가질 수 있으며, 네트워크 전체의 재구축이 필요하다고 CISA는 경고했다.

외부에서 별도의 침입을 필요로  
하지 않음



# 재택근무의 확산 – 보안위협 증대

[ 재택근무에 따른 주요 보안 위협 (출처 : 美 NIST) ]

구 분	주요 보안 위협
외부 단말기의 물리적 통제 미흡	<ul style="list-style-type: none"> <li>- 재택근무에 사용되는 외부 단말기의 분실·도난이나 타인의 정보 훔쳐보기 시 단말기 內 데이터가 유·노출</li> <li>- 외부 단말기를 통한 허가되지 않은 내부 네트워크 접근</li> </ul>
안전하지 않은 네트워크 사용	<ul style="list-style-type: none"> <li>- 공용 유무선 네트워크를 통해 내부망 접속 시 도청, 중간자 공격(MITM) 등으로 중요정보가 유출</li> </ul>
악성코드 감염에 따른 네트워크 침해	<ul style="list-style-type: none"> <li>- 악성코드에 감염된 외부 단말기로 내부 네트워크 연결 시 시스템 침해 가능</li> </ul>
내부 자원의 원격접근 위협	<ul style="list-style-type: none"> <li>- 내부에서만 접근 가능했던 내부 자원에 외부 단말기도 접근 가능해짐에 따라 비인가 접근 등 보안위협</li> </ul>

망분리환경에서 외부에서 내부로의 접근 경로가 만들어짐

# 다층방어체계-> 탐지(전파차단)의 중요성 증가



## 위협이 들어오지 못하게 방지

- 알려진 위협 대응 (백신, 패치 등)
- GPO기반 Hardening
- AI기반 탐지 (XDR, NDR, EDR 등)
- Infra ( F/W, IPS, IDS 등)
- Isolation , 망분리 등

## 내부전파를 최소화(차단, 탐지)

- 실시간 탐지 ( 보안관제 등 )
- 보안 감사
- 전파를 최소화 ( 접근통제 등)

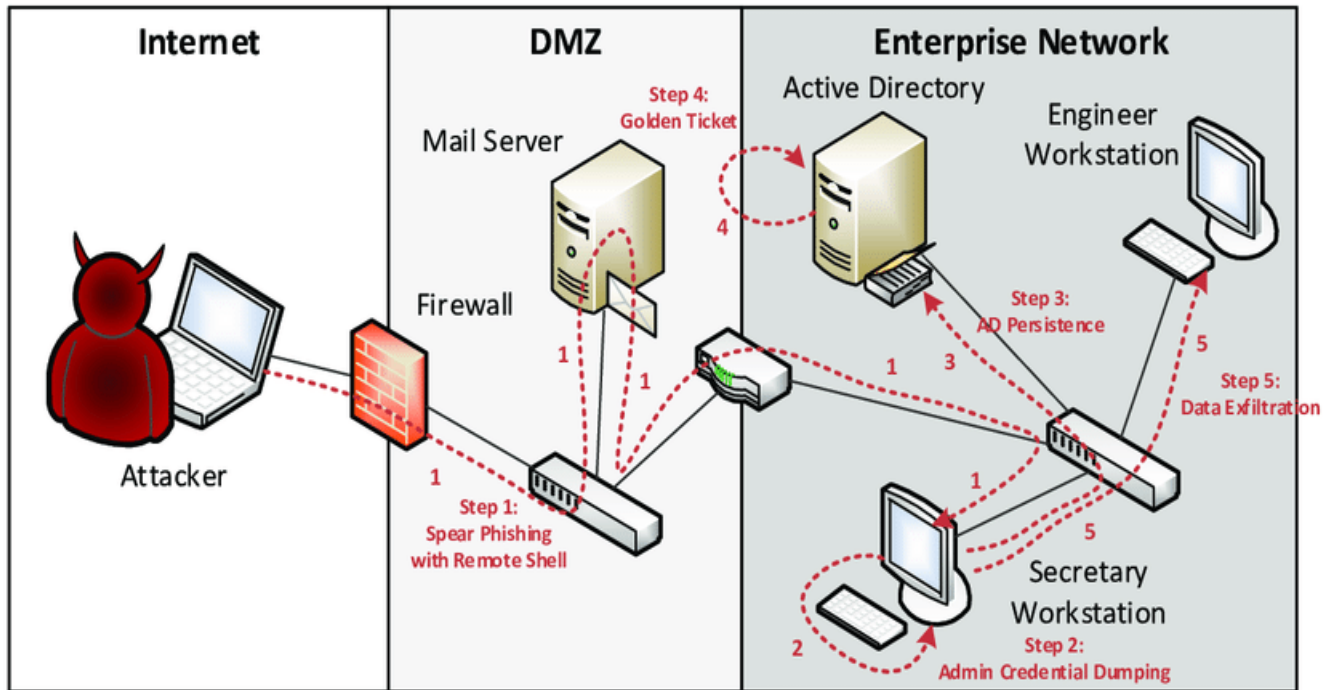
## 위협 이전으로 복구 및 분석

- 백업/복구
- 위협에 대한 분석



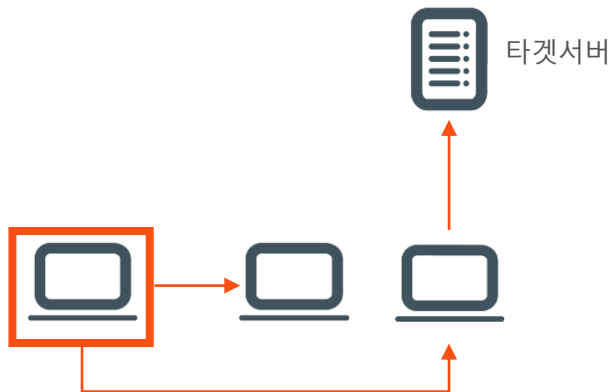
# 랜섬웨어 에서의 AD의 중요성과 사고사례

# 랜섬웨어의 일반적인 공격형태



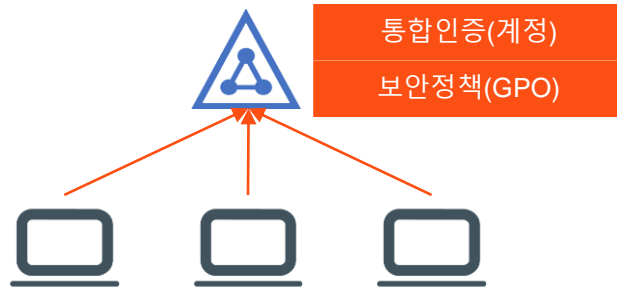
# 랜섬웨어의 타겟이 될 수밖에 없는 AD

## 랜섬웨어 전파형태



타겟 서버에 접근하기 위해서는 해당 서버에 접근할 수 있는 단말을 해킹 (접근통제로 제한된 접근 체계가 구성되어 있음)

## AD의 특징



모든 단말의 접근에 필요한 계정정보 및 보안정책을 관리하고  
모든 단말에 접근가능한 유일 통로  
GPO를 통해서 손쉽게 단말의 보안을 취약하게 설정 가능

# 국내주요 랜섬웨어 사고에서 AD는 주요 타겟

## [단독]SK하이닉스-LG전자 해킹... 기밀 대거 유출

서동원 기자, 홍세호 기자, 권도영 기자 | 입력 2020-09-10 03:00 | 수정 2020-09-10 03:00

해커단체, 불법인 랜섬웨어 공격  
반도체 전략 회의 등 자료 백가  
하이닉스-LG '보안대책 마련'

### SK하이닉스, LG전자 유출 자료 현황

	SK하이닉스	LG전자
자료 시점	주로 2013~2015년	주로 2016년, 2018년
공개된 자료 크기	597MB	50.1GB
자료 내용	<ul style="list-style-type: none"> <li>최고경영자(CEO) 보고 문건 다수</li> <li>해외 주요 고객사 관련 제안서</li> <li>미국 법인 현지 법무 대응 관련 내용</li> </ul>	<ul style="list-style-type: none"> <li>대부분 스마트폰 관련 프로그램 자료로 추정</li> <li>폴더명, 파일명 등으로 추정 가능한 관련 제품은 'V60(듀얼 스크린 스마트폰)', 'G800(벨벳 모델)' 등</li> </ul>

## Hackers target unpatched Citrix servers to deploy ransomware

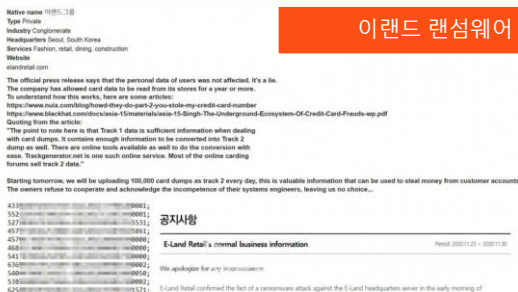
REvil ransomware gang has been spotted abusing Citrix bug to infect victims.

LG전자는 Citrix VDI를 통한 해킹

하이닉스는 채택근무 단말을 통한 해킹



quest.com | confidential



## [단독] 기아차 북미법인 이어 현대자동차그룹 내부자료 다크웹 유출됐다



제네시스 자동차도면 등 포함된 약 3,500여개 파일, 3.2GB 분량 다크웹에 유출

다크웹 주 무대로 활동하는 랜섬웨어 해커조직, 국내 대기업 타겟으로 장기간 공격 감행

## 보안공지

랜섬웨어 감염 확산에 따른 기업 보안점검 권고

KISA의 주요 대응 권고 문서

- ☑ 개요
  - ☑ 최근 기업 대상
  - ☑ 참고자료(www.boho.or.kr, 자료실)
  - ☑ 주요 사고 사례
  - ☑ 보안 상황
  - ☑ 대응 방안
  - ☑ 시사점
- 랜섬웨어 대응 가이드를 위한 안내 및 백업 가이드
    - 보호나라 홈페이지 → 자료실 → 가이드 및 매뉴얼 내 34번 게시물
  - 랜섬웨어 대응을 위한 안전한 정보시스템 백업 가이드
    - 보호나라 홈페이지 → 자료실 → 가이드 및 매뉴얼 내 35번 게시물
  - AD(Active Directory) 관리자가 피해자 할 6가지 AD운영 사례
    - 보호나라 홈페이지 → 자료실 → 보고서 내 213번 게시물
  - AD서버 악용 내부망 랜섬웨어 유포 사례 분석
    - 보호나라 홈페이지 → 자료실 → 보고서 내 215번 게시물
  - 최근 기업 대상 랜섬웨어 사고사례 및 대응방안
    - 보호나라 홈페이지 → 자료실 → 보고서 → 238번 게시물

Where Next Meets Now.

## 2. AD 보안을 위한 Quest의 솔루션

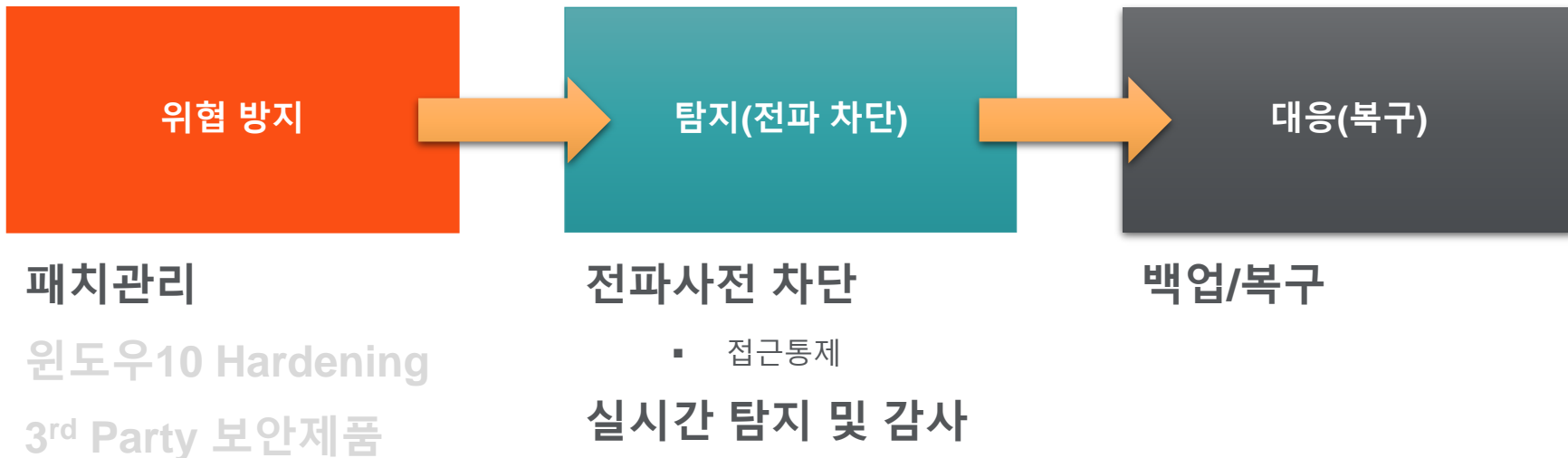
Quest

quest.com | confidential

Where Next Meets Now.



# 탐지 중심의 다층보안 체계





# Microsoft와의 AD보안 Co-Sell

클라우드 전환을 위한  
이메일 마이그레이션 및  
AD 기반 플랫폼 보안 고려사항

기업의 중요 커뮤니케이션 도구 중 하나인 메일 솔루션을 On-Premise 환경에서 클라우드로 전환을 고려 중인 기업이 많아지고 있습니다. 운영 비용의 절감과 업무 효율의 증가, 그리고 바이러스와 스펠을 차단하는 등 보안 위협에 보다 효과적으로 대비할 수 있기 때문인데요.

본 웨비나에서는 기업의 메일 솔루션을 Office 365 기반의 메일 솔루션(Exchange Online)으로 성공적으로 전환하는데 고려할 사항들을 소개합니다. 하이브리드 또는 클라우드로 전환을 위해서 고려할 사항들과 보안을 강화할 수 있는 방안들을 이번 웨비나에 참석하시어 확인하시길 바랍니다.

| 일시 |  
2019년 6월 4일 화요일 오후 3:00 - 4:00

| 아젠다 |

Content	Speaker
- 메일 마이그레이션 고려사항	마이크로소프트 김민정 과장
- 솔루션을 통한 Office 365로의 이메일 마이그레이션	퀘스트소프트웨어 채홍소 차장
- Hybrid, Cloud에서의 주요한 보안 고려사항	
- Hybrid, Cloud환경에서의 AD기반 플랫폼에 대한 보안 강화 방안	
- Q&A	

“여러분의 Active Directory는 안녕하십니까?”

증가하는 보안 위협,  
높아지는 Active Directory 중요성

최근에 급증하고 있는 Active Directory 보안 사고들...

관리자나 외부 신원에 의해서 발생하는 수많은 보안 및 서비스 위협들	2018년, 국내 A 기업에서 AD 서버 해킹으로 인한 전성택어 감염사고	2019년, 대만 컴퓨터 제조사인 아수스(ASUS) 공급망의 AD 서버 해킹으로 600여대 PC 감염	2019년, 사이버 범죄그룹 TAS05의 국내 기업들에 대한 AD-서버 해킹 시도 및 PC 감염 사고

귀사의 AD서버를 내/외부의 침해사고로부터 대비하십시오!

AD 서버 실시간 이상징후 탐지 및 대응

- 실시간 이상 로그인 행위 탐지
- 이상 권한 상승 행위 탐지
- 잘못된 변경 실시간 탐지
- 이상 및 해킹으로 인한 손상에 대한 데이터 기반의 빠른 복구

퀘스트는 On-Premise, Cloud, Hybrid Active Directory환경에 대한  
다양한 AD보안 솔루션을 제공합니다.

퀘스트 AD 보안 솔루션 웨비나 보기  
- Microsoft와 함께하는 Quest AD 보안이야기

웨비나 보기

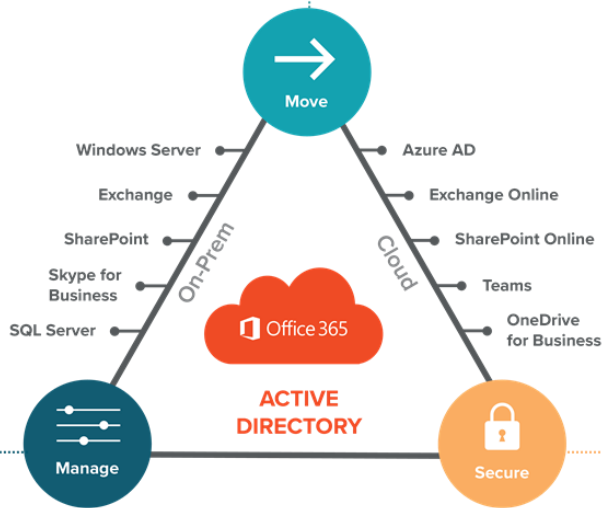


# Microsoft 플랫폼에 최적화된 토탈 솔루션 제공

<p><b>Migrate From:</b></p> <ul style="list-style-type: none"> <li>• Exchange</li> <li>• PSTs/Archives</li> <li>• Lotus Notes</li> <li>• Office 365</li> <li>• Active Directory</li> <li>• Windows Server</li> <li>• Gmail/G Drive</li> <li>• SharePoint</li> <li>• OneDrive</li> <li>• File shares</li> <li>• Box/Dropbox</li> <li>• Teams</li> </ul>	<p>→ Move Faster</p>	<p><b>Migrate To:</b></p> <ul style="list-style-type: none"> <li>• Office 365</li> <li>• Active Directory</li> <li>• Exchange</li> <li>• SharePoint</li> <li>• OneDrive for Business</li> <li>• Teams</li> </ul>
--	----------------------	--

## Stay in Control

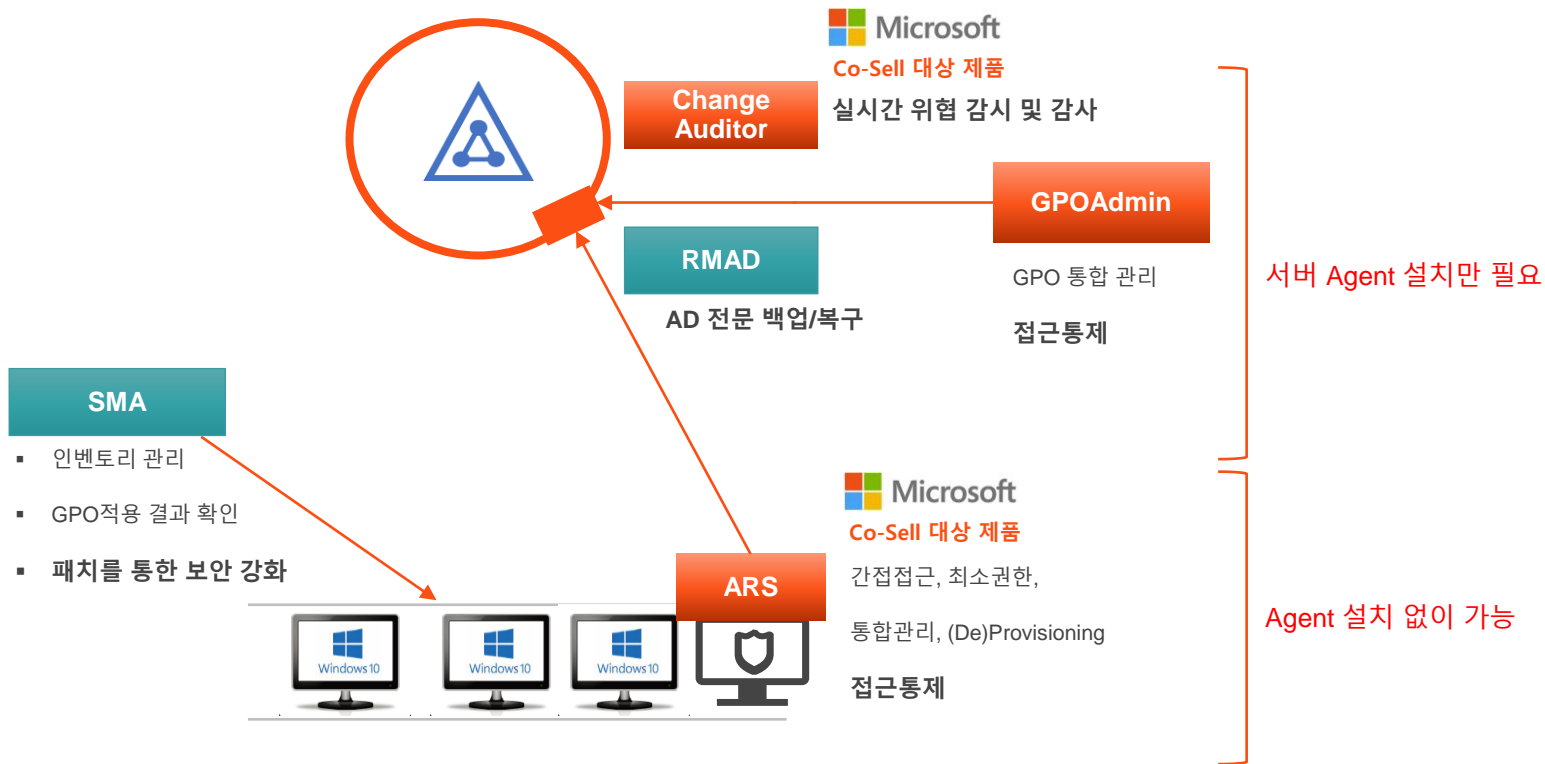
- Backup and recovery
- Reporting
- User and group management
- GPO management
- AD health and availability
- Office 365 license management



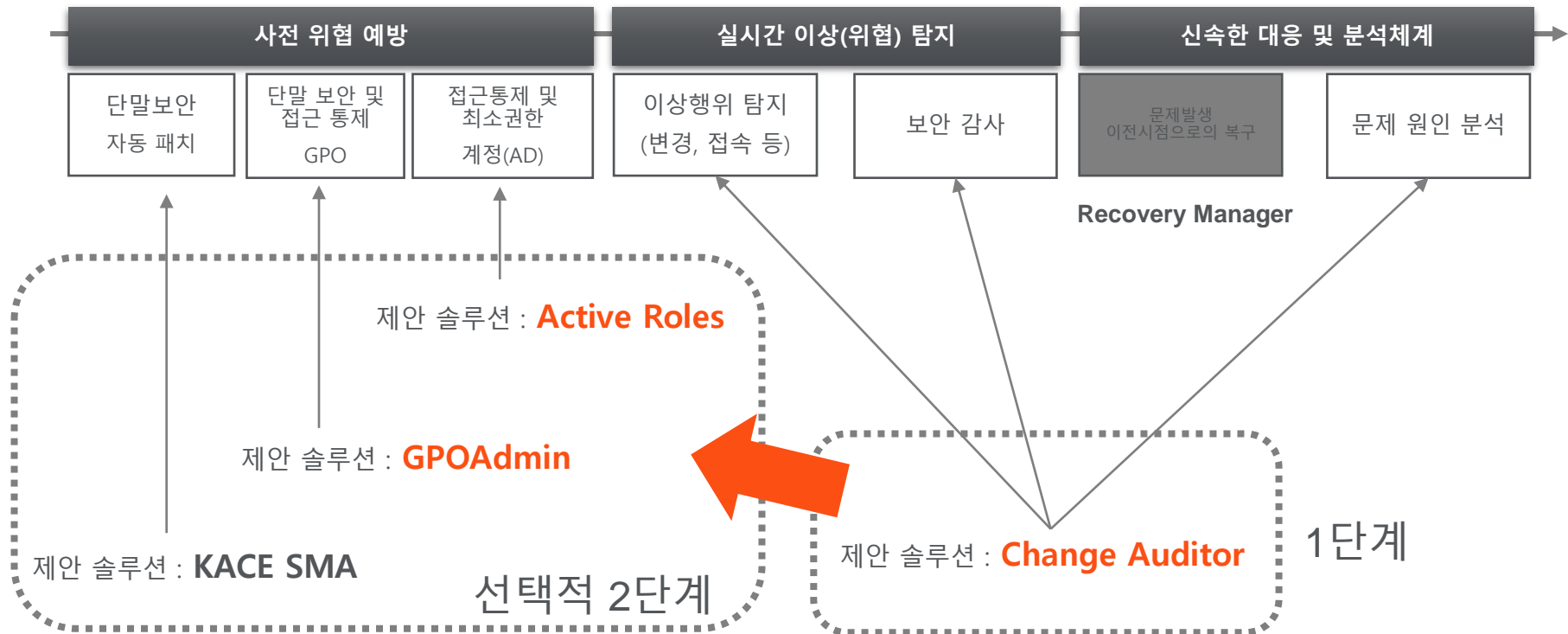
## Tighten Security

- Assess permissions to identify vulnerabilities
- Audit and alert on suspicious activity
- Remediate vulnerabilities and mitigate risk
- Investigate and recover from breaches

# 제품구성



# 퀘스트의 제안



# 3. 솔루션별 주요 기능





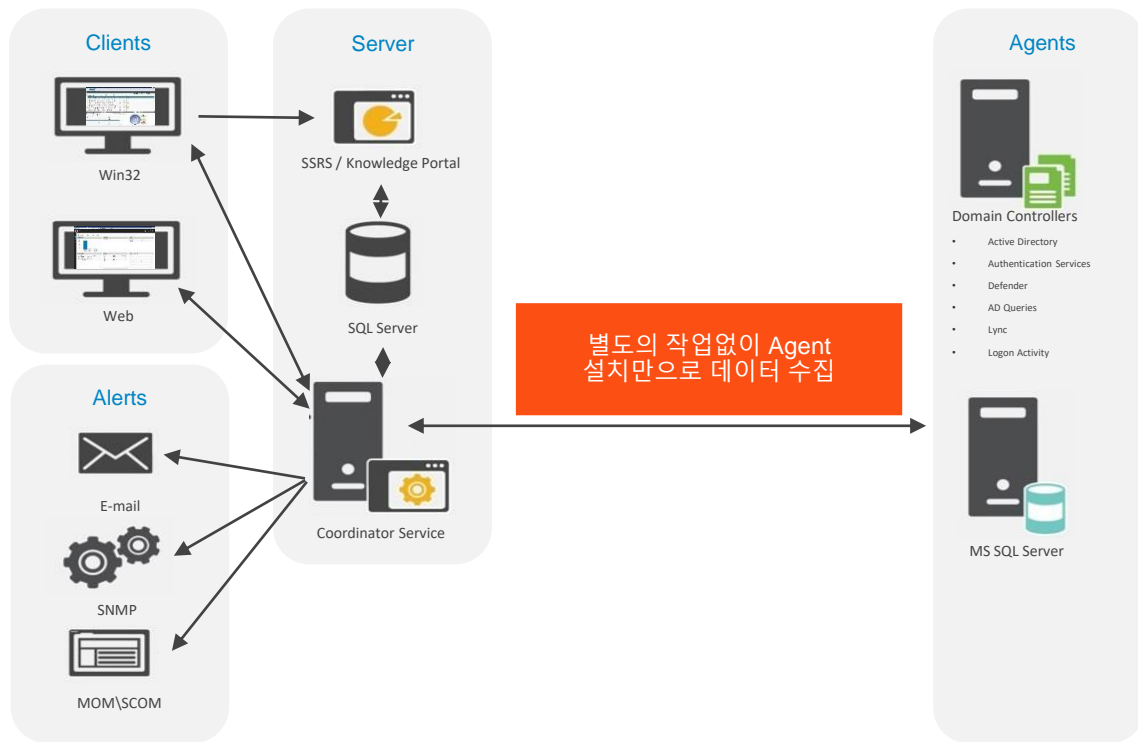
# 실시간 위협 탐지 솔루션

## - Change Auditor

# 다양한 형태의 정보를 제공



# 핵심 기능 - 위협분석을 위한 자체 데이터





# 핵심 기능 - 위협분석을 위한 자체 데이터

- Dynamic Access Control
- Connection Object
- Custom AD Object Monitoring
- Custom Computer Monitoring
- Custom Group Monitoring
- Custom User Monitoring
- DNS Service
- DNS Zone
- Domain Configuration
- Dynamic Access Control
- Forest Configuration
- FRS Service
- Group Policy Item
- Group Policy Object
- IP Security
- NETLOGON Service
- NTDS Service
- Organizational Unit (OU)
- Replication Transport
- Schema Configuration
- Site Configuration
- Site Link Bridge Configuration
- Site Link Configuration
- Subnets
- SYSVOL

## Configuration Monitoring

Table 1. Configuration Monitoring events

Event	Description	Severity
Active Directory Share Added	Created when an Active Directory share has been added to a server.	Medium
Active Directory Share Removed	Created when an Active Directory share has been removed from a server.	High
Append Parent Suffixes Option Changed	Created when the append parent suffixes of the primary DNS suffix option is changed.	Medium
Application Partition Replica Added	Created when a DN for an application partition is added to the msDS-hasMasterNCs attribute of an nTDSDSA object.	Medium
Application Partition Replica Removed	Created when a DN for an application partition is removed from the msDS-hasMasterNCs attribute of an nTDSDSA object.	High
Connection DNS Registration Option Changed	Created when the register connection in DNS option on a network connection is changed.	Medium
Connection Object Added	Created when an nTDSConnection object is added to the NTDS Settings container.	Medium
Connection Object Removed	Created when an nTDSConnection object is removed from the NTDS Settings container.	Medium
Connection-specific DNS Suffix Changed	Created when the connection-specific DNS suffix changes.	Medium
Contents of DNS Server List Changed	Created when a DNS server is added or removed from the DNS server list.	Medium
Contents of DNS Suffix List Changed	Created when a suffix is added or removed from the DNS suffix list.	Medium
Contents of WINS Server List Changed	Created when a server is added or removed from the WINS server list.	Medium
Critical Link Failures Allowed Parameter Changed	Created when the CriticalLink\alleresAllowed parameter on a DC is changed.	Medium
Default Gateway Changed	Created when the default gateway changes on a network connection.	Low
DHCP Disabled	Created when DHCP is disabled on a network connection.	Low
DHCP Enabled	Created when DHCP is enabled on a network connection.	Low
DIT Location Changed	Created when the directory path of the DIT is changed.	Low
Domain Controller Added as Preferred Bridgehead Server	Created when a domain controller is configured as a preferred bridgehead server for a particular replication transport.	Medium
Domain Controller Moved to Another OU	Created when a domain controller is moved to another OU.	Medium
Domain Controller Removed as Preferred Bridgehead Server	Created when a domain controller is removed as a preferred bridgehead server for a particular replication transport.	Medium
Domain Controller Service Pack Applied	Created when a service pack is applied to a domain controller.	Medium
Domain Controller Service Pack Rolled Back	Created when a service pack is removed from a domain controller.	Medium

- Authentication Activity
- Domain Controller Authentication
- Logon Session

## Authentication Activity

**IMPORTANT:** To capture Authentication Activity events, you must first enable (that is, set to Success/Failure) the 'Audit Logon events' audit policy for all servers and workstations.

Domain - Group Policy:

- Default Domain Policy\Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy\Audit logon events

Workgroup - Local Group Policy:

- Local Computer Policy\Computer Configuration\Windows Settings\Security Settings\Local Policies\Audit Policy\Audit logon events

**NOTE:** Authentication Activity events for servers are available with the Change Auditor for Logon Activity User auditing module. Authentication Activity events for workstations require the Change Auditor for Logon Activity Workstation auditing module and workstation agents to be deployed to the workstations to be monitored.

Table 1. Authentication Activity events

Event	Description	Severity
User failed to log on interactively	Created when a user failed to log on interactively to a computer. Windows Event equivalent: 529/4625	Medium
User failed to log on interactively from a remote computer	Created when a user failed to log on interactively from a remote computer. Windows Event: 529/4625	Medium
User failed to perform a network logon from a remote computer	Created when a user failed to log on from a remote computer on the network. (Disabled by default) Windows Event equivalent: 529/4625	Medium
User logged on interactively	Created when a user successfully logged on interactively to a computer. Windows Event equivalent: 528/4624 <b>NOTE:</b> When logging onto a monitored Windows 2012 or 2012 R2 server or a Windows 8 or 8.1 workstation, you may see additional events with "Windows Manager\WIM-vi" in the who information. This is expected behavior because the logon is being performed by the system.	Medium
User logged on interactively from a remote computer	Created when a user successfully logged on interactively from a remote computer. Windows Event equivalent: 528/4624	Medium
User performed a successful network logon from a remote computer	Created when a user successfully logged on from a remote computer on the network. (Disabled by default) Windows Event equivalent: 540/4624	Medium
User performed a successful NTLM V1 logon	Created when a user successfully logged into server through NTLM V1. (Disabled by default)	Medium
User performed a successful NTLM V2 logon	Created when a user successfully logged into server through NTLM V2. (Disabled by default)	Low

# 핵심 기능 - 모든 이벤트에 대한 위협도 제공

Drag a column header here to group by that column.

Severity	Facility Name	Event Class	Status	License Type	Subsystem	Results
Low	AD Query	AD Query Performed	Enabled	AD Query	AD Query	All Results
Low	Authentication Activity	User performed a successful NTLM V2 logon	Disabled	Logon Activity User	Logon Activity	All Results
Medium	Authentication Activity	User failed to log on interactively	Enabled	Logon Activity User	Logon Activity	All Results
Medium	Authentication Activity	User failed to log on interactively from a remote computer	Enabled	Logon Activity User	Logon Activity	All Results
Medium	Authentication Activity	User failed to perform a network logon from a remote computer	Disabled	Logon Activity User	Logon Activity	All Results
Medium	Authentication Activity	User logged on interactively	Enabled	Logon Activity User	Logon Activity	All Results
Medium	Authentication Activity	User logged on interactively from a remote computer	Enabled	Logon Activity User	Logon Activity	All Results
Medium	Authentication Activity	User performed a successful network logon from a remote computer	Disabled	Logon Activity User	Logon Activity	All Results
Medium	Authentication Activity	User performed a successful NTLM V1 logon	Disabled	Logon Activity User	Logon Activity	All Results
Medium	Authentication Services Monitoring	Authentication Services Computer Object Added	Enabled	Active Directory	Active Directory	All Results
Medium	Authentication Services Monitoring	Authentication Services Computer Object Attribute Changed	Enabled	Active Directory	Active Directory	All Results
Medium	Authentication Services Monitoring	Authentication Services Computer Object Deleted	Enabled	Active Directory	Active Directory	All Results
Medium	Authentication Services Monitoring	Authentication Services Computer Object Moved	Enabled	Active Directory	Active Directory	All Results
Medium	Authentication Services Monitoring	Authentication Services Computer Object Renamed	Enabled	Active Directory	Active Directory	All Results
Medium	Authentication Services Monitoring	Authentication Services GPO Setting Changed	Enabled	Active Directory	Active Directory	All Results
Medium	Authentication Services Monitoring	NIS Object Added	Enabled	Active Directory	Active Directory	All Results
Medium	Authentication Services Monitoring	NIS Object Attribute Changed	Enabled	Active Directory	Active Directory	All Results
Medium	Authentication Services Monitoring	NIS Object Deleted	Enabled	Active Directory	Active Directory	All Results
Medium	Authentication Services Monitoring	NIS Object Moved	Enabled	Active Directory	Active Directory	All Results
Medium	Authentication Services Monitoring	NIS Object Renamed	Enabled	Active Directory	Active Directory	All Results
Medium	Authentication Services Monitoring	Personality Object Added	Enabled	Active Directory	Active Directory	All Results
Medium	Authentication Services Monitoring	Personality Object Attribute Changed	Enabled	Active Directory	Active Directory	All Results
Medium	Authentication Services Monitoring	Personality Object Deleted	Enabled	Active Directory	Active Directory	All Results
Medium	Authentication Services Monitoring	Personality Object Moved	Enabled	Active Directory	Active Directory	All Results
Medium	Authentication Services Monitoring	Personality Object Renamed	Enabled	Active Directory	Active Directory	All Results
Medium	Authentication Services Monitoring	UNIX GEOS Changed	Enabled	Active Directory	Active Directory	All Results
Medium	Authentication Services Monitoring	UNIX Group ID Number Changed for Group	Enabled	Active Directory	Active Directory	All Results
Medium	Authentication Services Monitoring	UNIX Group ID Number Changed for User	Enabled	Active Directory	Active Directory	All Results
Medium	Authentication Services Monitoring	UNIX Group Name Changed	Enabled	Active Directory	Active Directory	All Results
Medium	Authentication Services Monitoring	UNIX Home Directory Changed	Enabled	Active Directory	Active Directory	All Results
Medium	Authentication Services Monitoring	UNIX Login Name Changed	Enabled	Active Directory	Active Directory	All Results
Medium	Authentication Services Monitoring	UNIX Login Shell Changed	Enabled	Active Directory	Active Directory	All Results
Medium	Authentication Services Monitoring	UNIX User ID Number Changed	Enabled	Active Directory	Active Directory	All Results
Medium	Authentication Services Monitoring	UNIX-Enabled Changed for Group	Enabled	Active Directory	Active Directory	All Results
Medium	Authentication Services Monitoring	UNIX-Enabled Changed for User	Enabled	Active Directory	Active Directory	All Results

High Level 위협은  
약 80개



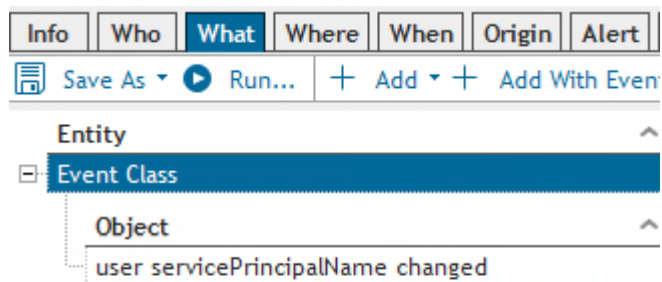
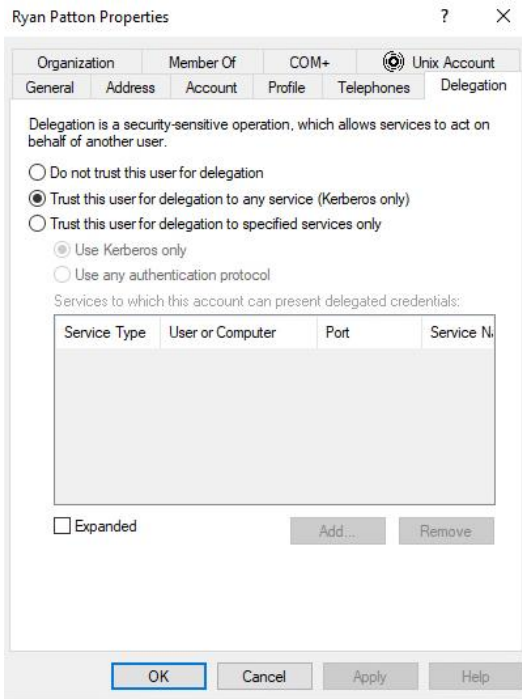
# 핵심 기능 - 정책기반의 위협 정의

The screenshot displays the Quest Change Auditor interface. The main window shows a search configuration for "Critical Group Membership changes in last 30 days". A red box highlights the search name and description fields. Below the main window, a detailed configuration panel is shown, also with a red box highlighting the "Info" tab and the "Save" and "Save As" buttons. The configuration panel includes fields for "Search Name", "Search Description", "Search Limit" (set to 50000), and "Refresh Interval" (set to 15 minutes).

Type	Alert	Report	Name	Alert To
Shared Search	-	-	Critical Group Membership changes in last 30 days	
Shared Search	-	-	Group membership changes in last 30 days	

→ 모든 형태의 조건 정의를 통해서 위협 정의 가능

# 핵심 기능 – 정책기반의 위협 정의(예시)



# 핵심 기능 - 실시간 알람 연동

The screenshot displays the Quest Change Auditor interface. The left pane shows a tree view of system categories, with 'Group Activity' selected. The main pane shows a table of alerts:

Type	Alert	Report	Name	Alert To	Alert Cc	Alert Bcc
<input checked="" type="checkbox"/>	Click here to filter data...					
<input checked="" type="checkbox"/>	Shared Search	-	Critical Group Membership changes in last 30 days			
<input checked="" type="checkbox"/>	Shared Search	-	Group Membership changes in last 30 days			

An 'Alert Custom Email' dialog box is open, showing configuration options:

- Send Alert To:  SNMP,  WMI,  SMTP
- Alert Subject: Change Auditor %ALERT\_TYPES% from %ALERT\_COORDINATOR\_NAME%: %ALER
- Send Plain Text Email:  Add Who,  Add Users,  Add Managers
- Send HTML Email:  To,  Cc,  Bcc

다양한 형태의 알람 연동

# 핵심 기능 - 분석 플랫폼 제공

The screenshot displays the Quest Configuration console. On the left, a tree view shows 'Administration Tasks' with sub-items like 'Coordinator', 'Agent', and 'Change Auditor Consumer Role'. The main pane shows 'Authorizations: Task' with a table of tasks and their definitions. A teal callout box with the text 'RBAC형태의 권한관리' (RBAC-style permission management) is overlaid on the task list. Below this, another teal callout box with the text '통합관리(설정)' (Integrated management (settings)) is overlaid on the configuration options.

The screenshot shows the Quest Change Auditor interface. At the top, it indicates the user is 'jqadmin' connected to 'MGMT1.questdemos.com'. Below is a table of events with columns for Severity, Time Detected, Subsystem, User, Event, and Computer. A teal callout box with the text '다양한 형태의 조회' (Diverse types of search) is overlaid on the bottom right of the interface. Below the table, a search filter configuration panel is visible, showing 'Selected Columns' and 'Order By' options.

Severity	Time Detected	Subsystem	User	Event	Computer	Action
High	2/18/2019 4:36 AM	Active Directory	questdemosDC15	Member removed from critical enterprise...	DC1	Delet
Medium	2/18/2019 4:36 AM	Active Directory	questdemosDC15	Nested member removed from critical ent...	DC1	Delet
High	2/18/2019 4:36 AM	Active Directory	questdemosDC15	Member removed from critical enterprise...	DC1	Delet
Medium	2/18/2019 4:36 AM	Active Directory	questdemosDC15	Nested member removed from critical ent...	DC1	Delet
High	2/18/2019 4:36 AM	Active Directory	questdemosDC15	Member removed from critical enterprise...	DC1	Delet
High	2/18/2019 4:36 AM	Active Directory	questdemosqadmin	Member added to critical enterprise group	DC1	Add A
High	2/18/2019 4:36 AM	Active Directory	questdemosqadmin	Member added to critical enterprise group	DC1	Add A
High	2/18/2019 4:36 AM	Active Directory	questdemosqadmin	Member added to critical enterprise group	DC1	Add A
High	2/18/2019 4:36 AM	Active Directory	questdemosqadmin	Member added to critical enterprise group	DC1	Add A



# 핵심 기능 - 보호기능

Change Auditor [connected to MGMT1.questdemos.com - DEFAULT] as user [qadmin (questdemos)]

File Edit Action View Help

Start Overview Searches Administration Tasks

Protection

Forest

- Active Directory (1)
  - ADAM (AD LDS) (0)
  - Group Policy (0)
- Applications
  - Exchange Mailbox (0)
- Server
  - File System (0)

Configuration

Auditing

Protection

Template	Status	Override Acc...	Objects	Override Account
Click here to filter data...				
Human Resources Protection Template	Enabled	Excluded fr...		

Object Canonical	Status	Object Class	Operations	Scope
Click here to filter data...				
questdemos.com/Users/Human_Resources	Enabled	group	Create, Delete, Modify Attributes	This object only

Attribute Protection

Click here to filter data...

Protect All

Override Account

Click here to filter data...

- questdemos\Administrator2
- questdemos\Administrator

Administration Account

Click here to filter data...

- questdemos\Administrator2
- questdemos/qadmin
- questdemos\Administrator

Active Directory Protection Wizard

(Optional) Select Accounts Allowed to Access Protected Objects:

Allow  Deny

Find: User, Computer, Group, ForeignSecuri

Name	Type
Click here to filter data...	
Administrator	User
Administrator2	User
Allowed RODC Password Replication Group	Security Group
ceo	User
Cert Publishers	Security Group
cio	User
Cloneable Domain Controllers	Security Group
DefaultAccount	User-Disabled
Denied RODC Password Replication Group	Security Group

36 Item(s) found.

Account

- questdemos.com/Users/Administrator2

Help Back Next Finish Cancel

# 핵심 기능 – SIEM연동

Change Auditor [connected to mgmt1.qdlab.local - DEFAULT] as user [QAdmin (QDLAB)]

The screenshot shows the Change Auditor web interface. The top navigation bar includes 'File', 'Edit', 'Action', 'View', and 'Help'. Below it are tabs for 'Start', 'Overview', 'Searches', 'All Active Directory Events', 'Deployment', and 'Administration Tasks'. The left sidebar is titled 'Configuration' and lists various settings: Agent, Coordinator, Purge and Archive (0), Private Alerts and Reports (0), SQL Reporting Services (0), Report Layouts (1), Application User Interface, Client Authentication, Threat Detection, On Demand Audit, and Event Subscriptions (0). A context menu is open over the 'Event Subscriptions' section, listing options: 'Add', 'Edit...', 'Delete...', and 'Refresh'. The 'Add' option is selected, showing a dropdown menu with 'ArcSight subscription...', 'QRadar subscription...', 'Splunk subscription...', and 'IT Security Search subscription...'. The 'Last Event' column is visible in the background table.

The 'Event Subscription Wizard' dialog box is shown, titled 'Configure Change Auditor to send events to Splunk'. It contains the following text: 'Provide the information required to send events to a Splunk instance.' Below this are two input fields: 'Destination URL' with instructions for Splunk Enterprise and Splunk Cloud, and 'Event Token' with a description of its purpose. At the bottom, there are buttons for 'Help', 'Back', 'Next', 'Finish', and 'Cancel'.

일반적인 Syslog 형태의 연결도 지원



# 주요 활용 #1. 정책기반 위협 감시

운영과정에서  
실수나 /  
관리문제로 인하여  
발생하는 보안  
이슈

내부자나 외부  
인력에 위한 위협  
감시

정상적인 행위처럼  
수행되는 내역에  
대해서도 감시

Info	Who	What	Where	When	Origin	Alert	Report	Layout	
Save	Save As	Run...	+ Add	+ Add With Events	Delete Criteria	Edit Event Class...			
Entity	Exclude	Action(s)	Transport(s)	Port					
Event Class	False								
Object	Restriction								
Local user added									
UNIX-Enabled User Created									
User added									
User object added									
Viral user created									

# 주요활용 #2. 알려진 위협 감시

알려진 위협에  
대한 감시

▲ Medium Severity

Who: THUNDERREALM\Administrator  
Where: DC01  
What: nTDSDSA Thunderrealm.com/Configuration/Sites/Default-First-Site-Name/Servers/THUNDERWKS/NTDS Settings changed  
Active Directory  
Class: nTDSDSA  
Object: Thunderrealm.com/Configuration/Sites/Default-First-Site-Name/Servers/THUNDERWKS/NTDS Settings

Source: Change Auditor  
Action: Delete Object  
Attr:

When: 9/17/2020 10:07:18 AM  
Origin: thunderwks.Thunderrealm.com...  
Result: Success  
Facility: Custom AD Object Monitoring  
Authentication: Kerberos  
Port: 389

▲ Medium Severity

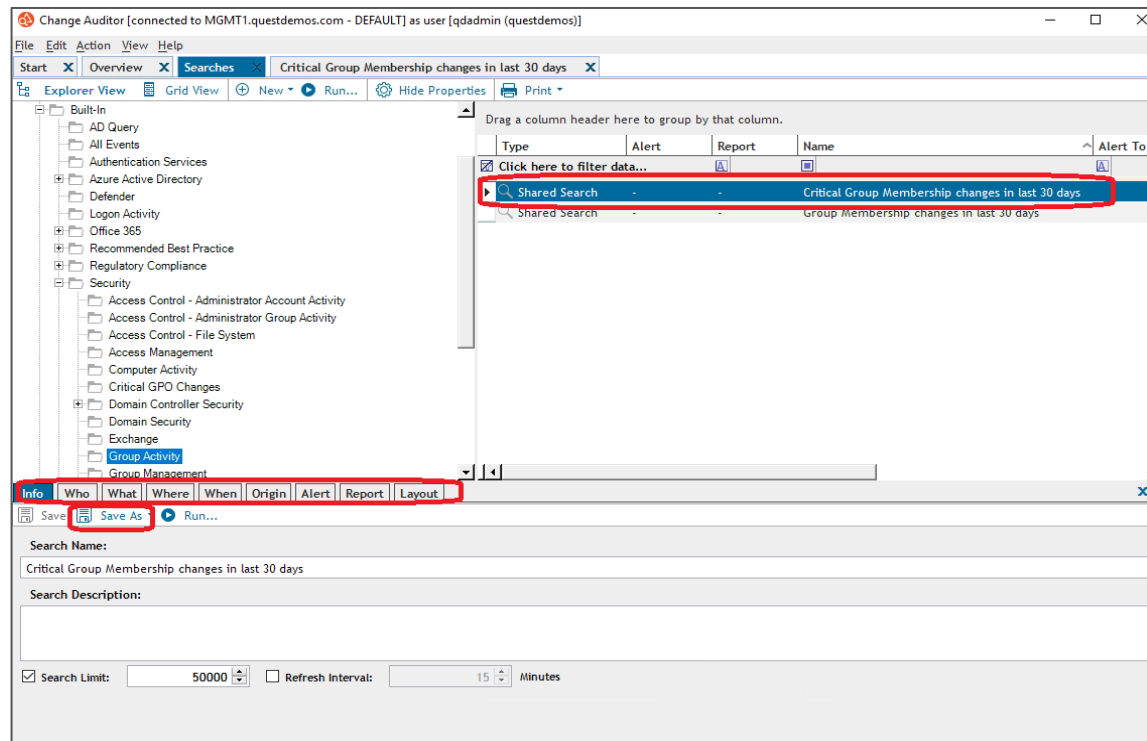
Who: THUNDERREALM\Administrator  
Where: DC01  
What: servicePrincipalName attribute was changed for computer Thunderrealm.com/Enterprise/Computers/UnitedStates/THUNDERWKS  
Active Directory  
Class: computer  
Object: Thunderrealm.com/Enterprise/Computers/UnitedStates/THUNDERWKS

Source: Change Auditor  
Action: Add Attribute  
Attr: servicePrincipalName

When: 9/17/2020 11:38:42 AM  
Origin: thunderwks.Thunderrealm.com...  
Result: Success  
Facility: Custom AD Object Monitoring  
Authentication: Kerberos  
Port: 389

From: <Not Set>  
To: GC/thunderwks.Thunderrealm.com/Thunderrealm.com

# 주요 활용 #3. 분석 체계 마련 및 가시성 확보

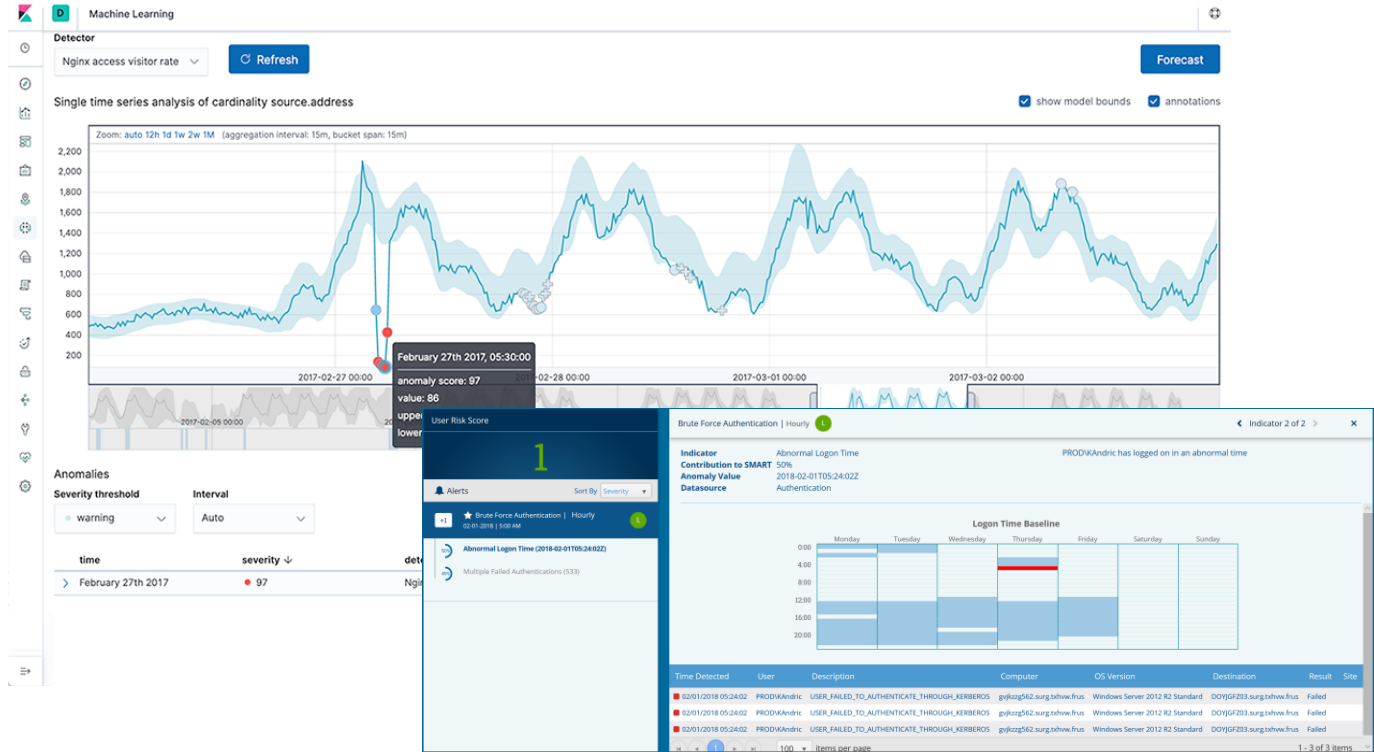


모든 데이터의 DB화 및 확장된 검색을  
통한 분석 체계 제공

정의된 리포트를 통해서 원하는  
데이터를 손쉽게 조회

# 주요 활용 #4. SIEM연동을 통한 데이터분석

데이터 전처리  
형태로 SIEM에  
필요한 데이터를  
제공

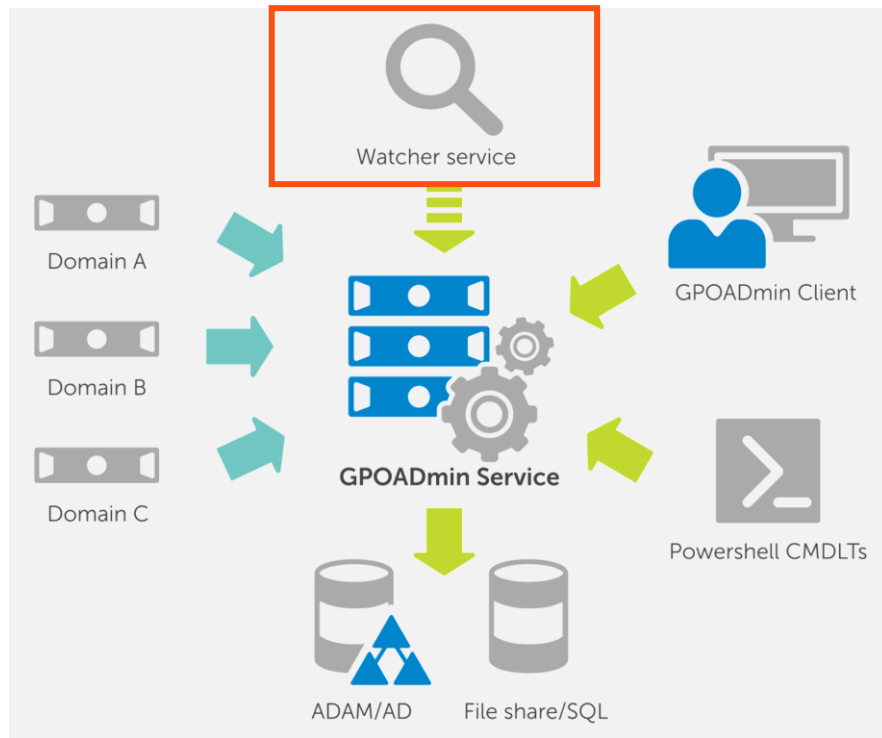




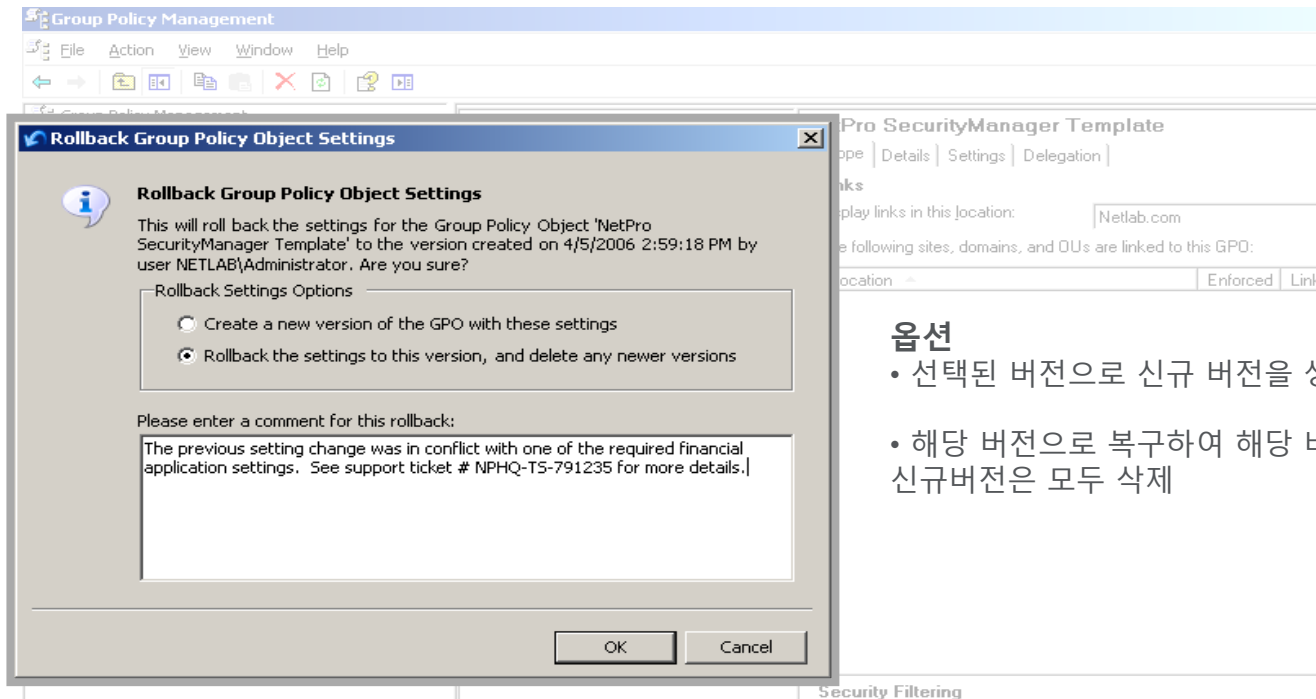
# GPO 통합관리 및 접근통제

## - GPOAdmin

# 핵심 기능 – Watcher를 통한 이상 생성 감시



# 핵심 기능 – GPO 즉시 복구



## 옵션

- 선택된 버전으로 신규 버전을 생성
- 해당 버전으로 복구하여 해당 버전 이후 신규버전은 모두 삭제

# 핵심 기능 – 자동 버전 관리

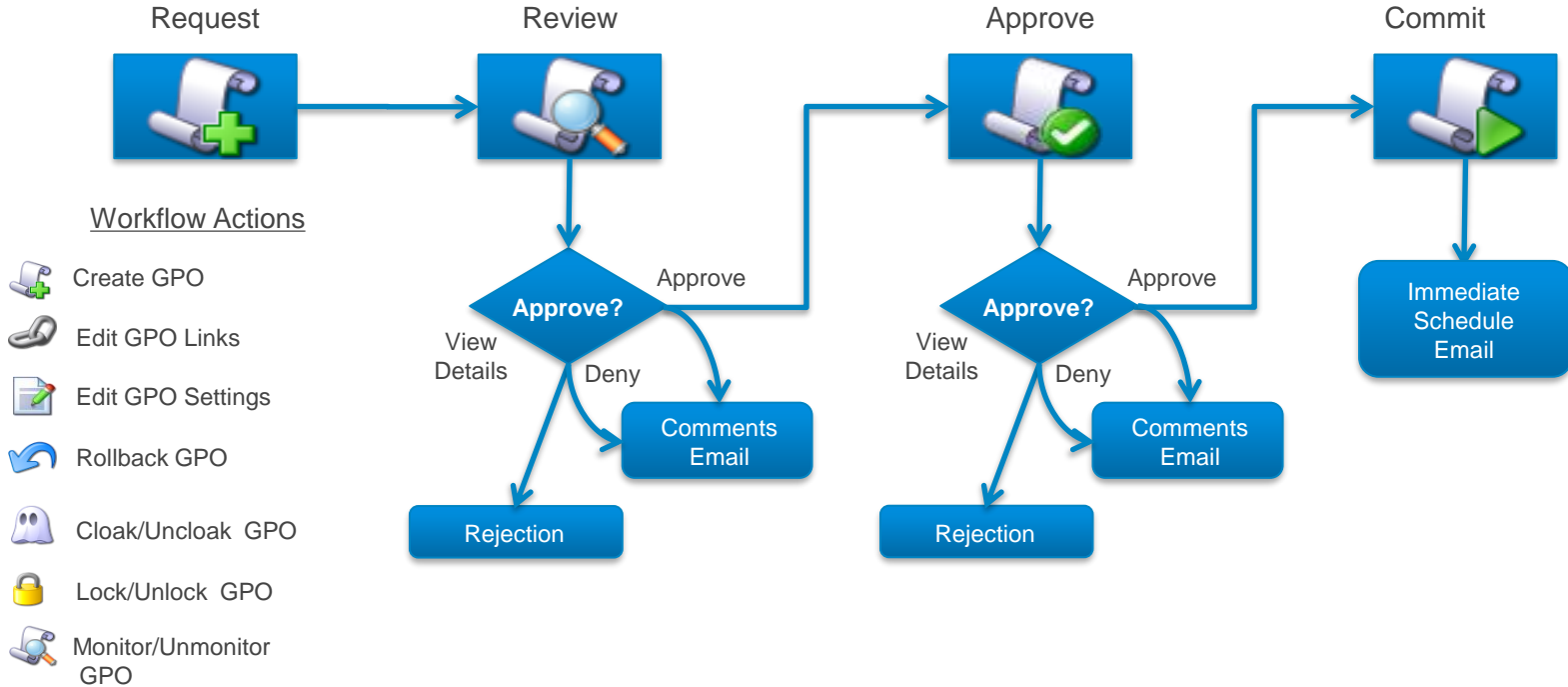
The screenshot displays the 'Group Policy Objects in NPPM.LOCAL' window. It features a toolbar with 'Edit', 'Workflow', 'Cloak', 'Lock', 'Register', and 'Reports' options. Below the toolbar is a table listing various Group Policy Objects (GPOs) with their respective 'Register Status' and 'Version'.

Name	Register Status	Version
ADMIN Preferences	Registered	5.1
ADMINS POLICY	Registered	1.2
Corporate Users GPO	Registered	7.0
Default Domain Controllers Policy	Registered	2.0
Default Domain Policy	Registered	2.0
LoopBack Policy		
Policy Preferences	Registered	1.1
Service Accounts Policy	Registered	1.0
TEST	Registered	1.1
TEST LOGON SCRIPT		

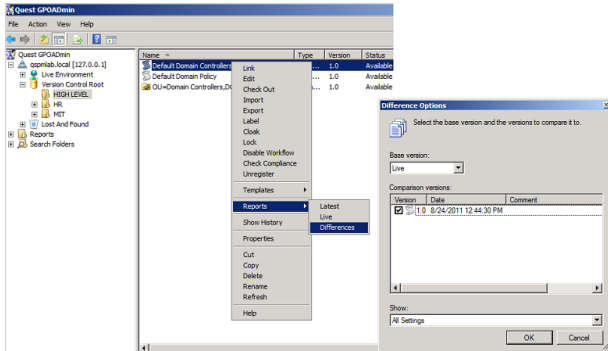
A 'Check Out: Corporate Users GPO' dialog box is overlaid on the bottom right. It contains the text 'Enter a comment for this action' and a text input field. At the bottom of the dialog are 'OK' and 'Cancel' buttons.



# 핵심 기능 – 승인기반 Workflow



# 핵심 기능 - 버전별 자동 비교



**Differences Report**

**Group Policy Object Difference Report**

Comparing: Corporate Users GPO (WorkingCopy-Cloaked)  
 With: Default Domain Policy (Live)  
 Data collected on: 11/25/2016 5:21 AM

**Summary:**  
 15 items added  
 5 items removed  
 6 items changed

General	Corporate Users GPO (WorkingCopy-Cloaked)	Default Domain Policy (Live)
Name	Corporate Users GPO	Default Domain Policy
Version	WorkingCopy-Cloaked	Live
Creation Time	Friday, November 25, 2016 5:18:50 AM	Thursday, November 3, 2016 9:52:31 AM
Modified Time	Friday, November 25, 2016 5:20:31 AM	Friday, November 25, 2016 4:57:49 AM
Read Time	Friday, November 25, 2016 5:21:38 AM	Friday, November 25, 2016 5:21:50 AM
Identifier	{DE088DA5-5881-480E-8204-53205881A90B}	{3182F340-016D-11D2-945F-00C04FB984F9}
Domain	Gpoadmin2016.dev.hal.ca.qstf	GPOAdmin2016.dev.hal.ca.qstf
Owner		
	<b>Status</b>	<b>Corporate Users GPO (WorkingCopy-Cloaked)</b>
Name	Unchanged	GPOADMIN2016\administrator
SID	Unchanged	S-1-5-21-4258997743-2570352427-4241420526-500
	<b>Status</b>	<b>Default Domain Policy (Live)</b>
Name		GPOADMIN2016\administrator
SID		S-1-5-21-4258997743-2570352427-4241420526-500
	<b>Status</b>	<b>Corporate Users GPO (WorkingCopy-Cloaked)</b>
Trustee		
Name	Removed	GPOADMIN2016\administrator
SID	Removed	S-1-5-21-4258997743-2570352427-4241420526-500
Trustee	Added	
Name	Added	NT AUTHORITY\Authenticated Users
SID		S-1-5-11
	<b>Status</b>	<b>Default Domain Policy (Live)</b>
	<b>Status</b>	<b>Corporate Users GPO (WorkingCopy-Cloaked)</b>
	<b>Status</b>	<b>Default Domain Policy (Live)</b>
Permission		
Name	Unchanged	GPOADMIN2016\administrator
Allowed Permissions	Unchanged	Edit, delete, modify security
Allowed Permissions	Changed	Edit, delete, modify security
Inherited	Unchanged	Apply Group Policy
Permission		
Name	Added	NT AUTHORITY\Authenticated Users
Allowed Permissions	Added	Apply Group Policy



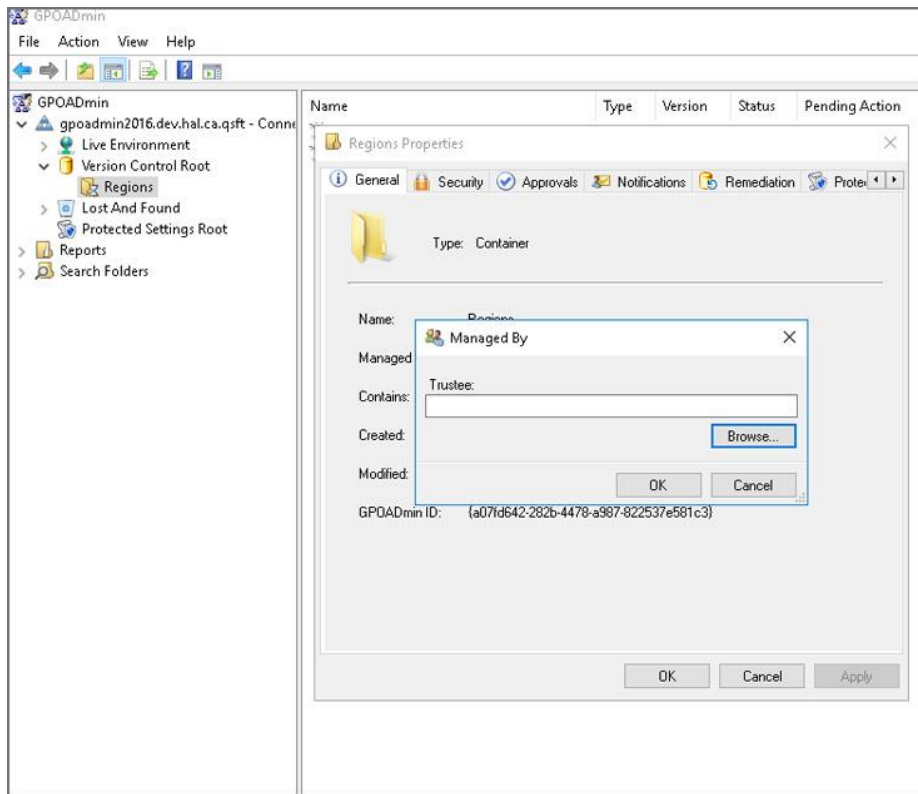
# 핵심 기능 – GPO 숨김 및 보호

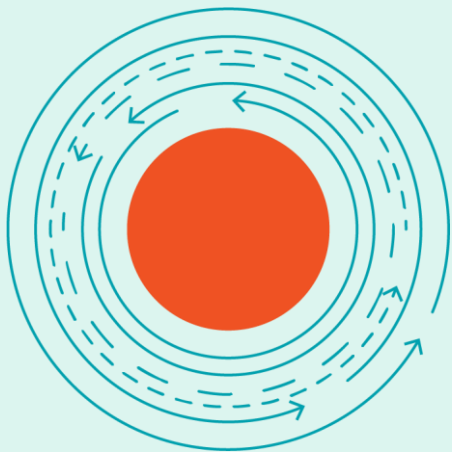
The screenshot displays the Group Policy Management console for the Netlab.com domain. The left pane shows the tree structure with 'Group Policy Objects' expanded. The right pane, titled 'Group Policy Objects in Netlab.com', shows a list of GPOs with columns for Name, User, Monitored, Locked, and Cloaked. The 'Test- Office 2003 Policy' is highlighted, showing it is Monitored, Locked, and Cloaked.

Name	User	Monitored	Locked	Cloaked
Default Domain Controllers Policy		Yes	Yes	No
Default Domain Policy		Yes	No	No
Finance		Yes	No	No
NetPro SecurityManager Template		Yes	No	No
New Group Policy Object		Yes	No	No
New Group Policy Object2		Yes	No	No
<b>Test- Office 2003 Policy</b>		Yes	Yes	Yes

# 핵심 기능 – GPO별 담당자 지정

최소권한 관리를 통한 보안 향상  
관리 효율성 재고

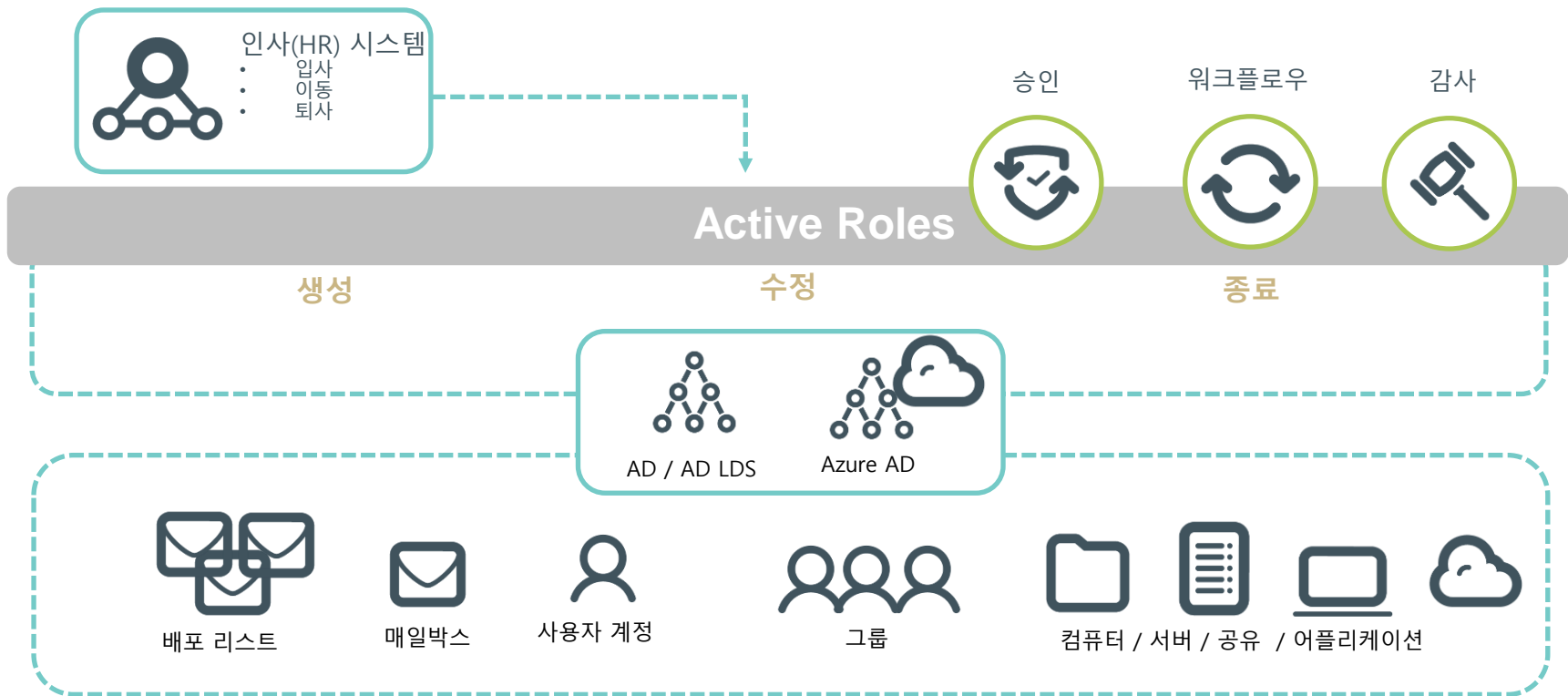




# 계정 접근통제 및 통합관리

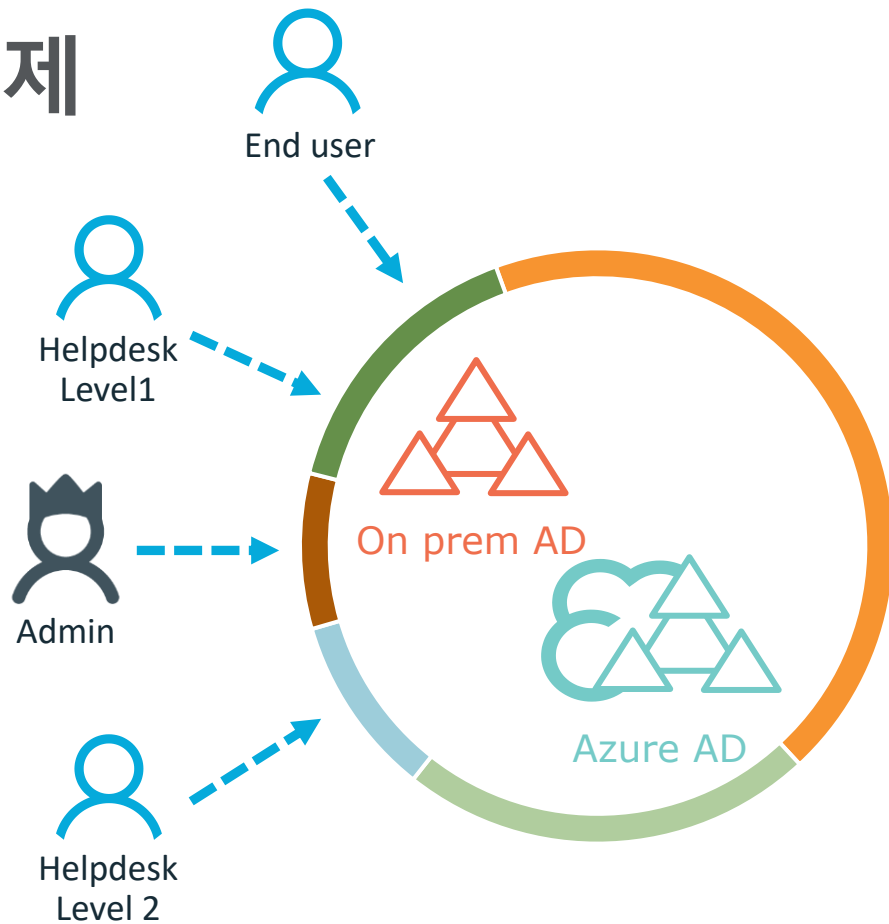
## - Active Roles

# AD 통합 관리



# 핵심 기능 - AD 접근통제

- 최소 권한 관리
- 접근 통제
- 통합 관리
- 기존 윈도우 계정권한의 간소화 및 이를 통한 보안위협 제거



# 핵심 기능 – 관리자 노출 위험성을 최소화

- Active Directory / Azure
- Exchange / Office 365
- SharePoint / Online
- Skype for Business

The screenshot displays the Active Roles console for 'demoapp.demolab.com'. The left pane shows a tree view of configuration options, with 'Advanced' under 'Active Directory' selected. The right pane shows a list of permissions for 'Users'.

Name
Users - Read/Write Account Information
Users - Read/Write Account Restrictions
Users - Read/Write Dial-In Properties
Users - Read/Write General Information
Users - Read/Write Logon Information
Users - Read/Write Organizational Information
Users - Read/Write Personal Information
Users - Read/Write Phone and Mail Options
Users - Read/Write Profile Properties
Users - Read/Write Public Information
Users - Read/Write Web Information
Users - Read/Write WTS Properties
Users - Rename
Users - Reset Password (Extended Right)
Users - Run Check Policy (Extended Right)
Users - Undo Deprovision
Users - Undo Deprovision - Deny



# 핵심 기능 - 완벽한 사용자 라이프사이클 관리

인사(HR)시스템

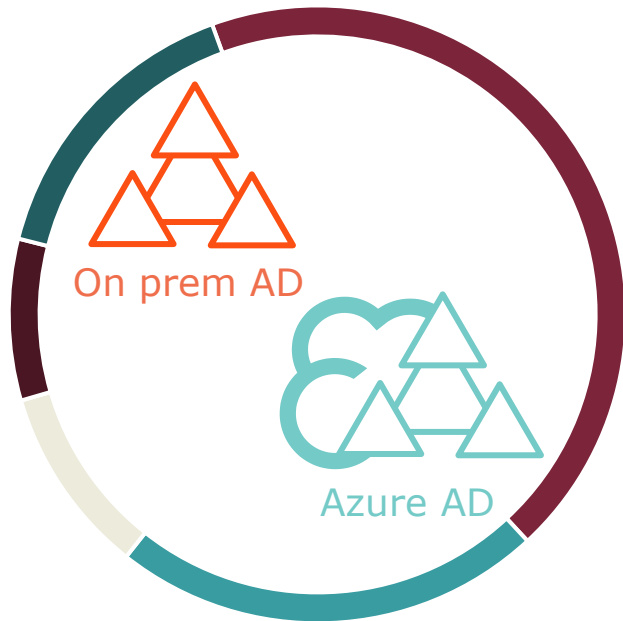
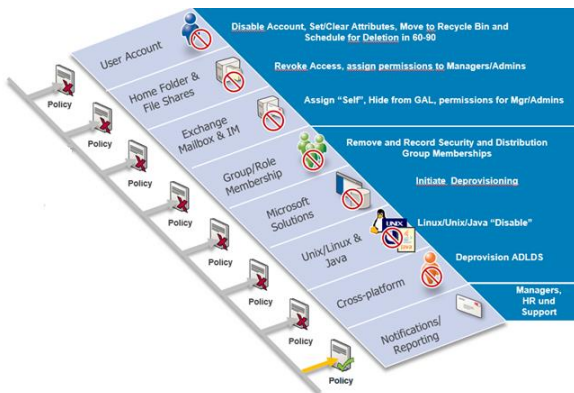
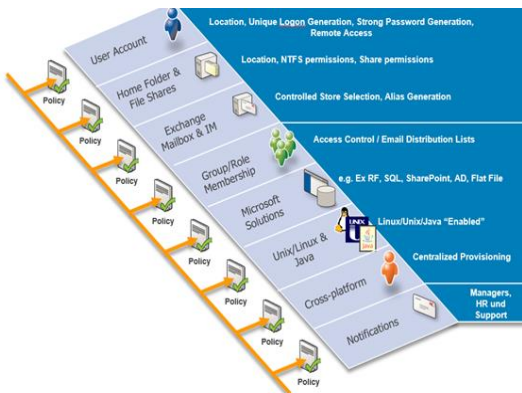
- 입사
- 이동
- 퇴사



완벽한 사용자 라이프사이클 관리

프로비저닝  
외부 계정 자동 생성

디-프로비저닝  
외부 계정 자동 제거



O365와 Cloud기반 SaaS서비스도 지원

# 핵심 기능 - 워크플로우 엔진

## ■ 사용자 정의 자동화된 워크플로우

- 작업에 대한 요청을 승인처리
- GUI기반의 워크플로우 엔진 제공을 통한 손쉽게 생성
- 워크플로우 기반의 관리를 통해서 프로세스의 자동화

The screenshot displays the Quest workflow engine interface. At the top, the title is "Notification of managed object excess (Template)". Below the title, there is a warning icon and the text "This workflow is disabled." followed by instructions: "Drag activities to the surface on the right." A search bar with the placeholder "Type a name to find" is present. The left sidebar contains two main categories: "Basic activities" and "Object management". Under "Basic activities", there are buttons for "Notification", "Script", "If-Else", "Stop/Break", and "Add Report Section". Under "Object management", there are buttons for "Search" and "Stop Search". The main workspace shows a workflow diagram with a start node (green arrow) leading to a "Check object count" activity. This activity has two outgoing paths: "Count exceeds the threshold" leading to a "Send notification" activity, and "No excess" leading to a "Drop Activities Here" activity. Both paths converge at a red stop icon. At the bottom right, there are three buttons: "Run Workflow", "Save Changes", and "Discard Changes".

# 핵심기능 - 모든 변경 내역을 제공

- Active Roles내에서 발생한 모든 변경 기록 정보를 제공

모든 변경 기록정보 제공으로 자체적인

보안감사 및 이슈 분석 가능

The screenshot displays the Active Roles console interface. On the left is a navigation pane with options like Home, Directory Management, Search, Customization, Approval, Settings, and Help. The main area shows the user profile for 'Reto Bachmann - Zuerich' and a list of operations. Two operations are visible:

Operation ID	Requested by	Completed
1-156	ONEIDENTITY\Administrator	11/6/2016 8:10:14 PM (UTC)
1-152	ONEIDENTITY\Administrator	11/6/2016 8:07:03 PM (UTC)

Each operation entry includes details such as the user name, reason, and a table of property changes with old and new values.



# Thank You

Quest  
Where Next Meets Now.