AD기반 단말 환경에서의 랜섬웨어 예방 및 실시간 탐지 전략

Solution Consultant

Hongso Chae(Hongso.chae@quest.com)

Quest

Where Next Meets Now.

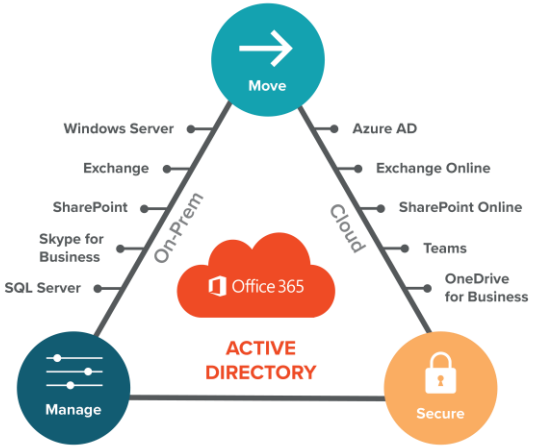
회사소개

Quest는 빠르게 변화하는 엔터프라이즈 IT 환경을 위한 소프트웨어 솔루션을 제공합니다.

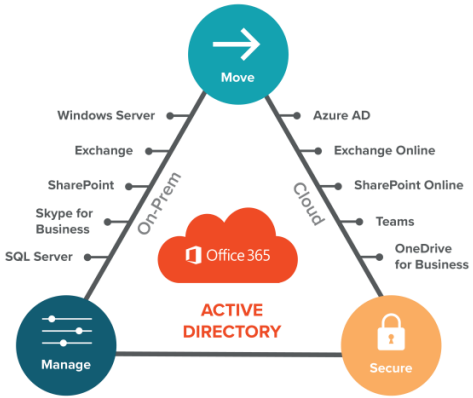
Quest는 데이터 폭발, 클라우드 확장, 하이브리드 데이터 센터, 보안 위협 및 규정 요구사항으로 인한 문제를 단순화할 수 있도록 지원하며 Fortune 500 대 기업의 95%와 Global 1000 대 기업의 90%를 포함하여 100 개국 130,000여 기업에 글로벌 서비스를 제공하고 있습니다.

Data Management	**Microsoft Platform**	Data Protection	Unified Endpoint Management	IAM

2년 연속 Microsoft 최우수 Global ISV



Quest Security Solution Overview

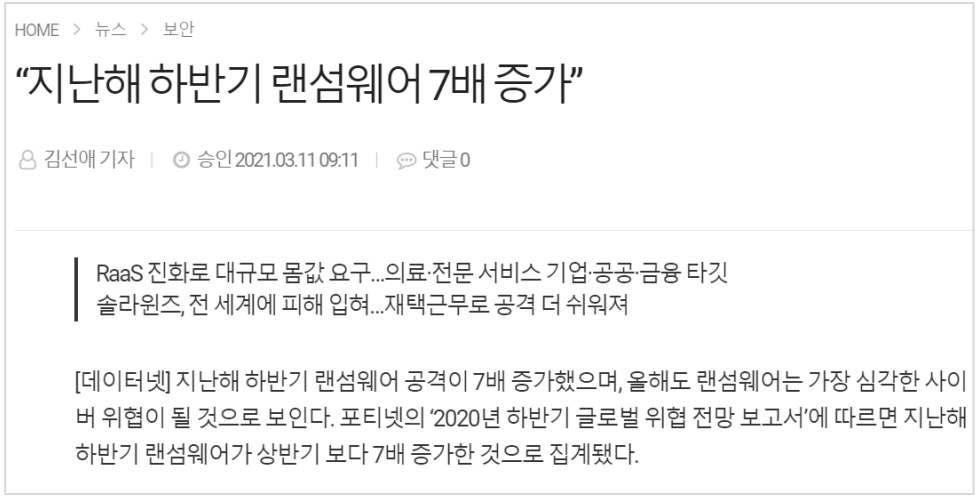


AD 보안 (랜섬웨어 전파 차단 및 실시간 탐지)	• GPO 접근통제 및 통합관리 : **GPOAdmin** • AD 계정 접근통제 및 통합관리 : **Active Roles** • 실시간 위협 탐지 및 감사 : **Change Auditor for AD**, Exchange 등 • 복구 솔루션 : Recovery Manager for AD
통합 패스워드 관리	• 통합 시스템,네트워크,어플리케이션 패스워드 관리: **One Identity Safeguard Password**
스트리밍 기반의 기록 및 녹화	• 기록 및 녹화(Citrix 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 #정보보안 #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

- 데이터 암호화
- 데이터 탈취
- 디도스 공격

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

솔리윈즈 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 침임을 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	- 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

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

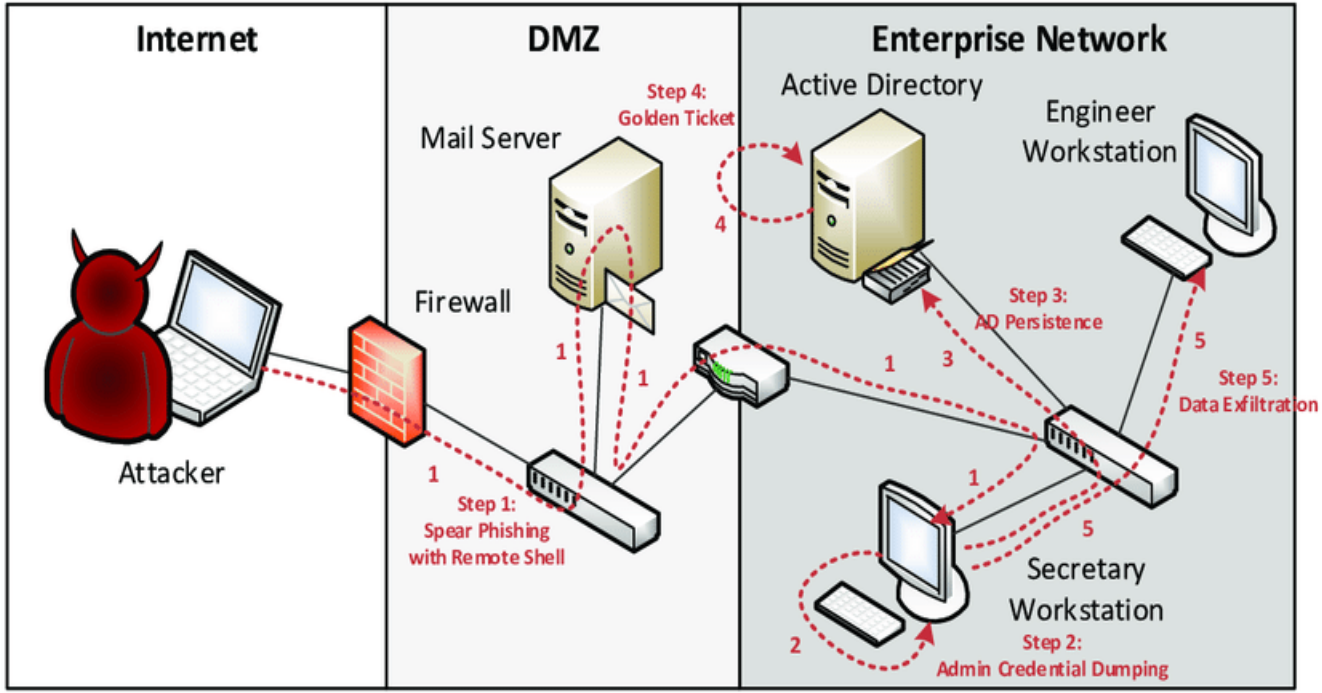
- 백업/복구
- 위협에 대한 분석

랜섬웨어 에서의 AD의 중요성과 사고사례

Quest

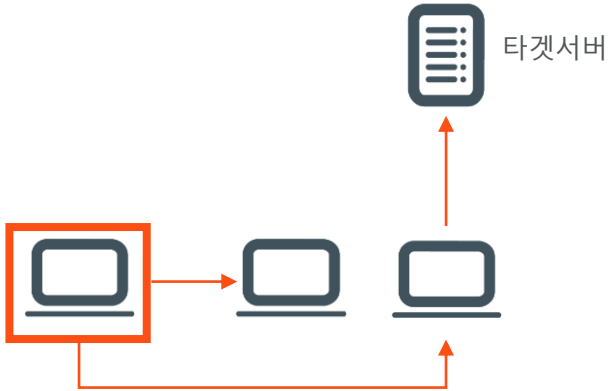
Where Next Meets Now.

랜섬웨어의 일반적인 공격형태



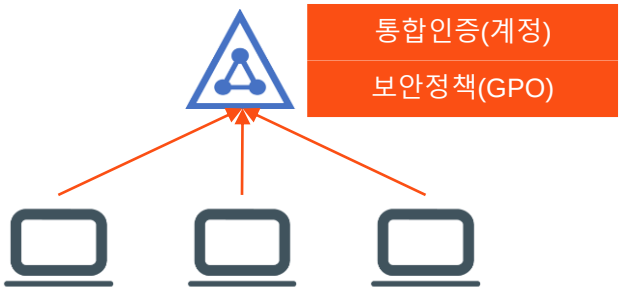
랜섬웨어의 타겟이 될 수밖에 없는 AD

랜섬웨어 전파형태



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

AD의 특징

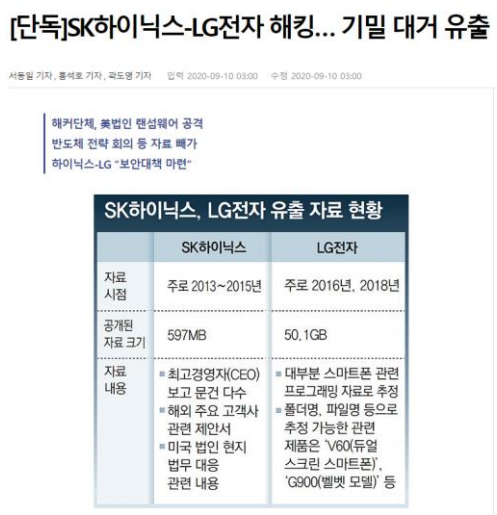


모든 단말의 접근에 필요한 계정정보 및 보안정책을 관리하고

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

서동일 기자, 홍석호 기자, 곽도영 기자 입력 2020-09-10 03:00 수정 2020-09-10 03:00

해커단체, 美법인 랜섬웨어 공격
반도체 전략 회의 등 자료 빼가
하이닉스-LG "보안대책 마련"

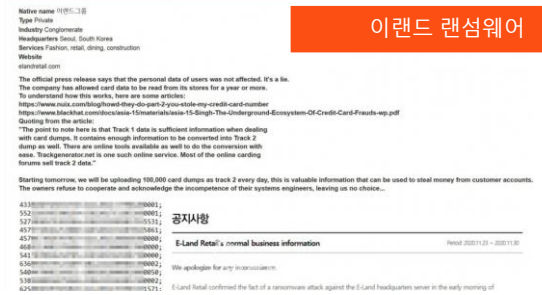
SK하이닉스, LG전자 유출 자료 현황

	SK하이닉스	LG전자
자료 시점	주로 2013~2015년	주로 2016년, 2018년
공개된 자료 크기	597MB	50.1GB
자료 내용	▪ 최고경영자(CEO) 보고 문건 다수 ▪ 해외 주요 고객사 관련 제안서 ▪ 미국 법인 현지 법무 대응 관련 내용	▪ 대부분 스마트폰 관련 프로그래밍 자료로 추정 ▪ 폴더명, 파일명 등으로 추정 가능한 관련 제품은 'V60(듀얼 스크린 스마트폰)', 'G900(벨벳 모델)' 등


>_ CL0P^_- LEAKS

HOME IHI-CSI.DE MVTEC.COM NFT.CO.UK POLYVLIES.DE INRIX.COM EXECUPHARM.COM TWL.DE RFRANCO.COM
PLANATOL.DE HOEDLMAYR.COM INDIABULLS.COM PROMINENT.COM NETZSCH.COM PRETTL.COM SOFTWAREAG.COM
TAMINTL.COM ALLSTATEPETERBILT.COM NOVABIOMEDICAL.COM PARKLAND.CA ELANDRETAIL.COM

이랜드 랜섬웨어


Native name 이랜드그룹
Type Private
Industry Conglomerate
Headquarters Seoul, South Korea
Services Fashion, retail, dining, construction
Website
elandretail.com

The official press release says that the personal data of users was not affected. It's a lie.
The company has allowed card data to be read from its stores for a year or more.
To understand how this works, here are some articles:
https://www.nuix.com/blog/how-they-do-part-2-you-stole-my-credit-card-number
https://www.blackhat.com/docs/asia-15/materials/asia-15-Singh-The-Underground-Ecosystem-Of-Credit-Card-Frauds-wp.pdf
Quoting from the article:
"The point to note here is that Track 1 data is sufficient information when dealing with card dumps. It contains enough information to be converted into Track 2 dump as well. There are online tools available as well to do the conversion with ease. Trackgenerator.net is one such online service. Most of the online carding forums sell track 2 data."

Starting tomorrow, we will be uploading 100,000 card dumps as track 2 every day, this is valuable information that can be used to steal money from customer accounts. The owners refuse to cooperate and acknowledge the incompetence of their systems engineers, leaving us no choice...

공지사항

E-Land Retail's normal business information

We apologize for any inconvenience.

E-Land Retail confirmed the fact of a ransomware attack against the E-Land headquarters server in the early morning of


보안공지

랜섬웨어 감염 확산에 따른 기업 보안점검 권고

KISA의 주요 대응 권고 문서

□ 참고자료(www.boho.or.kr, 자료실)
(1) 랜섬웨어 대응 가이드을 위한 안내 및 백업 가이드
- 보호나라 홈페이지 → 자료실 → 가이드 및 매뉴얼 내 34번 게시물
(2) 랜섬웨어 대응을 위한 안전한 정보시스템 백업 가이드
- 보호나라 홈페이지 → 자료실 → 가이드 및 매뉴얼 내 35번 게시물
(3) AD(Active Directory) 관리자가 피해야 할 6가지 AD운영 사례
- 보호나라 홈페이지 → 자료실 → 보고서 내 213번 게시물
(4) AD서버 악용 내부망 랜섬웨어 유포 사례 분석
- 보호나라 홈페이지 → 자료실 → 보고서 내 215번 게시물
(5) 최근 기업 대상 랜섬웨어 사고사례 및 대응방안
- 보호나라 홈페이지 → 자료실 → 보고서 → 238번 게시물

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 재택근무 단말을 통한 해킹

[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 타깃으로 장기간 공격 감행

2. AD 보안을 위한 Quest의 솔루션

탐지 중심의 다층보안 체계

패치관리

윈도우10 Hardening

3rd Party 보안제품

전파사전 차단

- 접근통제

실시간 탐지 및 감사

백업/복구

Microsoft와의 AD보안 Co-Sell

Microsoft Quest

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 스팸을 차단하는 등 보안 위협에 보다 효과적으로 대비할 수 있기 때문인데요.

본 웨비나에서는 기업의 메일 솔루션을 Office 365 기반의 메일솔루션(Exchange Online)으로 성공적으로 전환하는데 고려할 사항들을 소개합니다. 하이브리드 또는 클라우드 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 - Hybrid, Cloud에서의 주요한 보안 고려사항 - Hybrid, Cloud환경에서의 AD기반 플랫폼에 대한 보안 강화 방안	퀘스트소프트웨어 채홍소 차장
- Q&A	

Quest Microsoft

"여러분의 Active Directory는 안녕하십니까?"

**증가하는 보안 위협,
높아지는 Active Directory 중요성**

최근에 급증하고 있는 Active Directory 보안 사고들…

관리자나 외부 인력에 의해서 발생하는 수많은 보안 및 서비스 위협들

2018년, 국내 A 기업에서 AD 서버 해킹으로 인한 랜섬웨어 감염사고

2019년, 대만 컴퓨터 제조사인 아수스(ASUS) 공급망의 AD 서버 해킹으로 600여대 PC 감염

2019년, 사이버 범죄그룹 TA505의 국내 기업들에 대한 AD서버 해킹 시도 및 PC 감염 사고

귀사의 AD서버를 내/외부의 침해사고로 부터 대비하십시오!

Quest
Change Auditor for AD

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

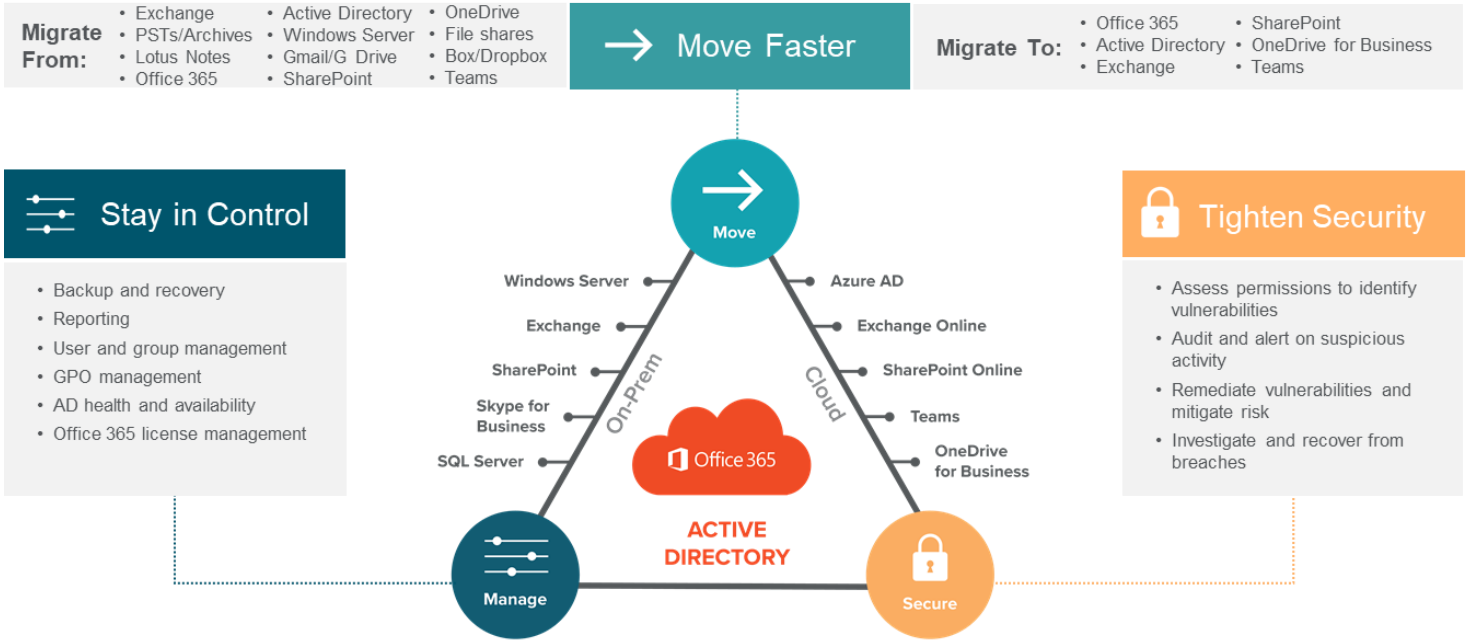
- Microsoft와 함께하는 Quest AD 보안이야기

웨비나 보기

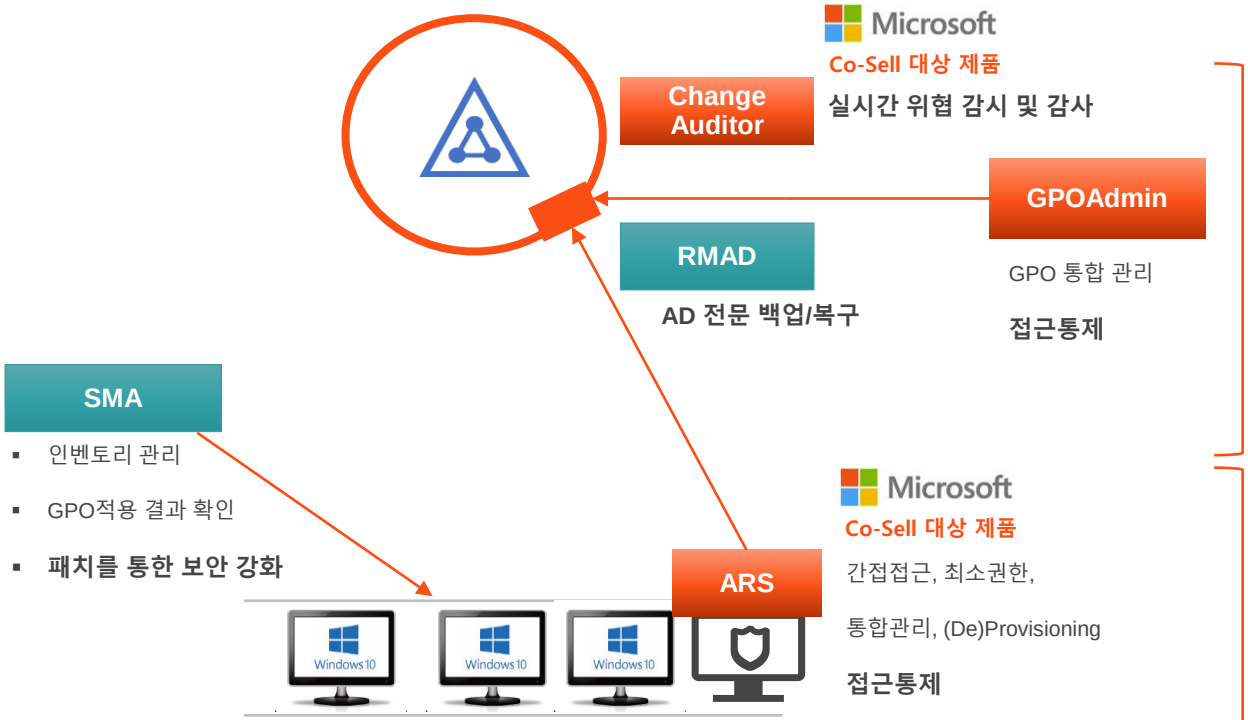
Quest

Where Next Meets Now.

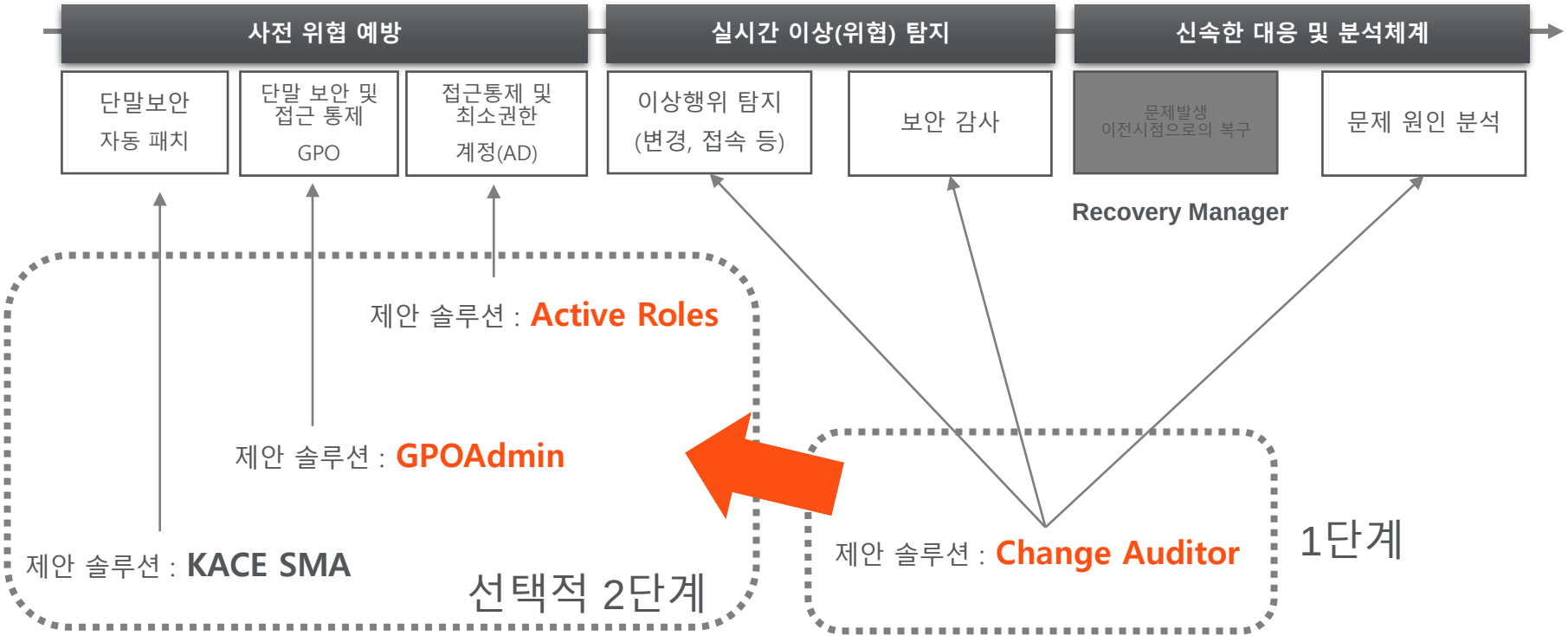
Microsoft플랫폼에 최적화된 토탈 솔루션 제공



제품구성



퀘스트의 제안


사전 위협 예방
실시간 이상(위협) 탐지
신속한 대응 및 분석체계
단말보안
자동 패치
단말 보안 및
접근 통제
GPO
접근통제 및
최소권한
계정(AD)
이상행위 탐지
(변경, 접속 등)
보안 감사
문제발생
이전시점으로의 복구
문제 원인 분석
Recovery Manager
제안 솔루션 : Active Roles
제안 솔루션 : GPOAdmin
제안 솔루션 : KACE SMA
선택적 2단계
제안 솔루션 : Change Auditor
1단계

3. 솔루션별 주요 기능

실시간 위협 탐지 솔루션

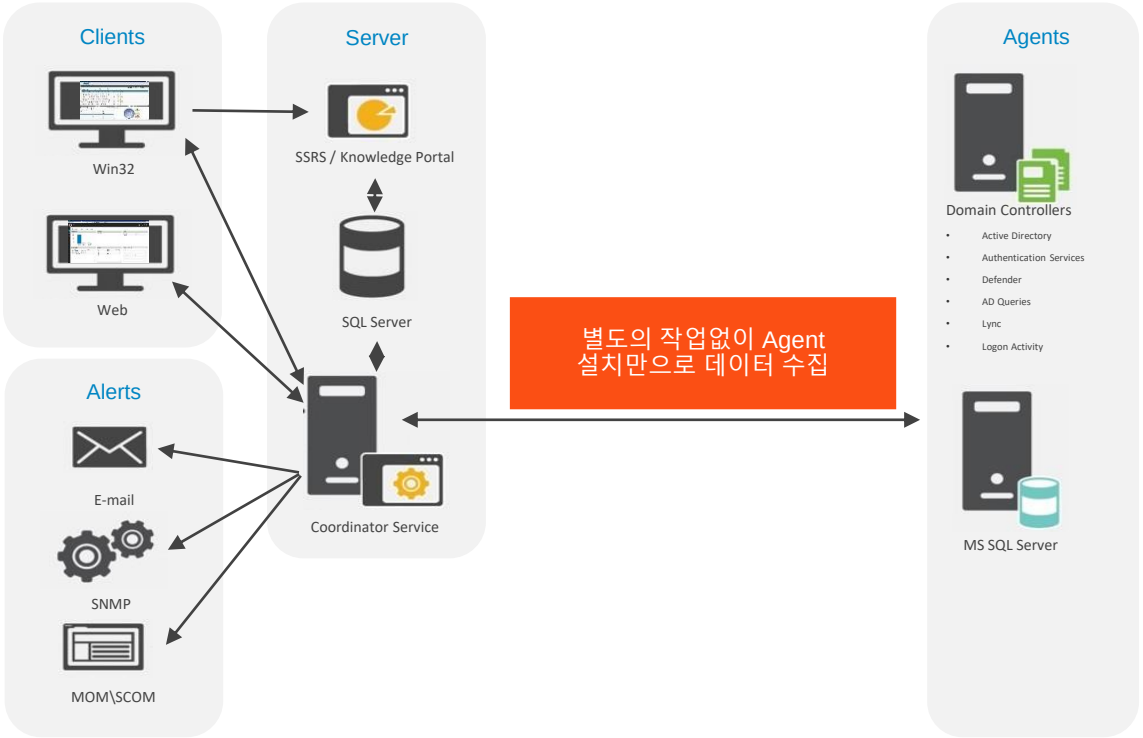
- Change Auditor

Quest

Where Next Meets Now.

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 CriticalLinkFailuresAllowed 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 **NOTE:** 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\DWM-n' 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	Crated 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

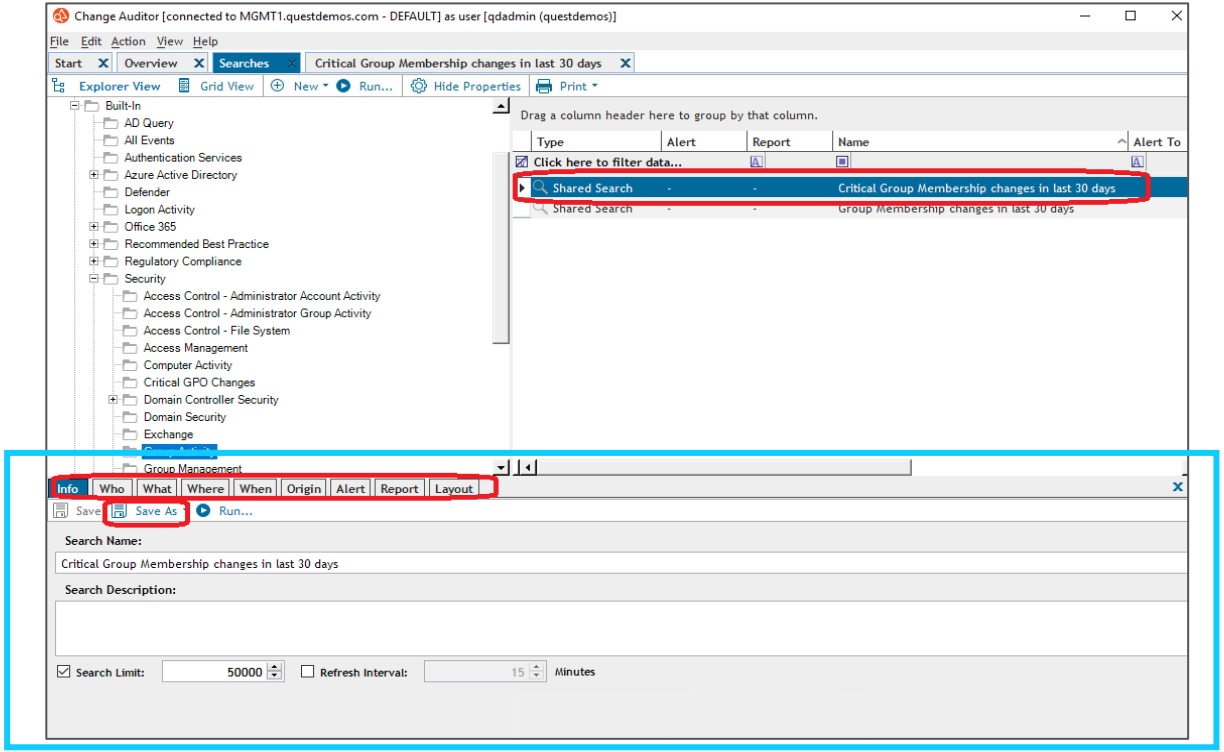
Edit... | High | Medium | Low | Enable | Disable | Default | Knowledge Base... | Print

Drag a column header here to group by that column.

Severity	Facility Name	Event Class	Status	License Type	Subsystem	Results
Click here to filter data...						
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 GECOS 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

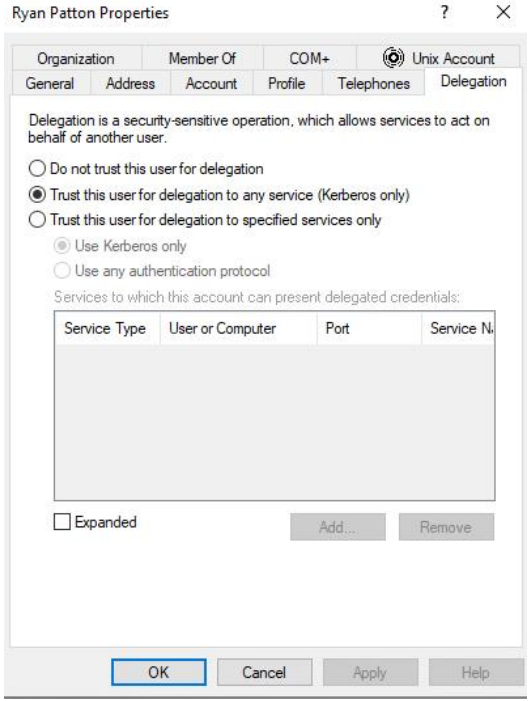
High Level위협은 약 80개

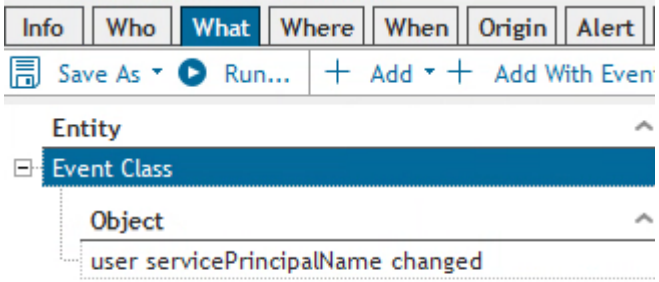
핵심 기능 – 정책기반의 위협 정의



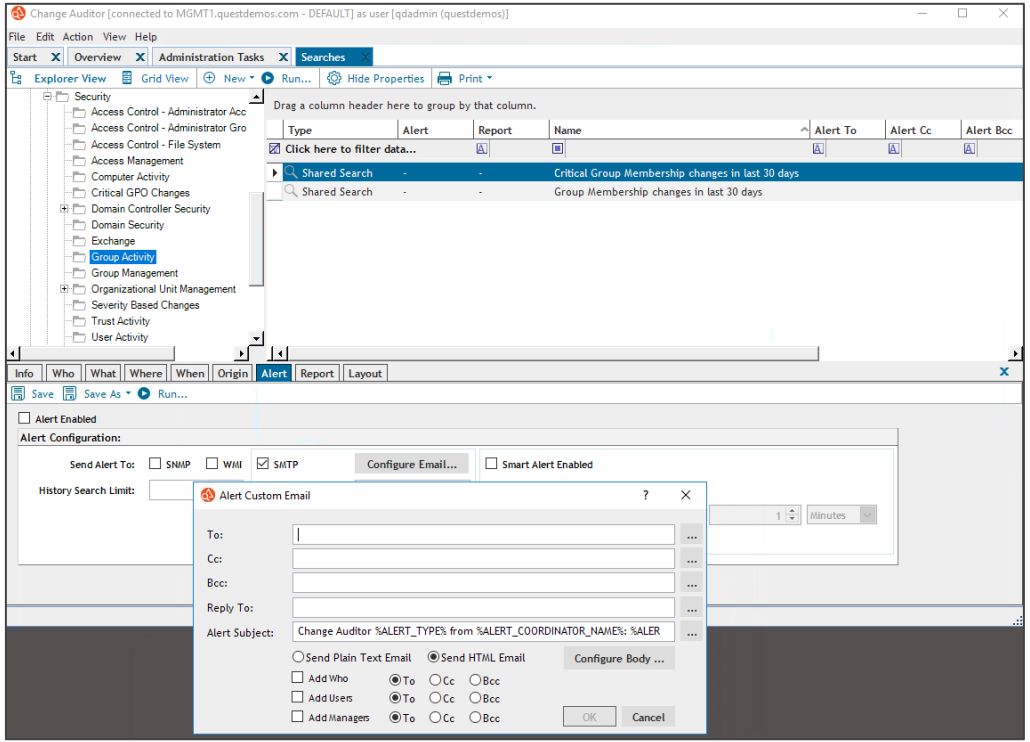
모든 형태의 조건 정의를
통해서 위협 정의 가능

핵심 기능 – 정책기반의 위협 정의(예시)



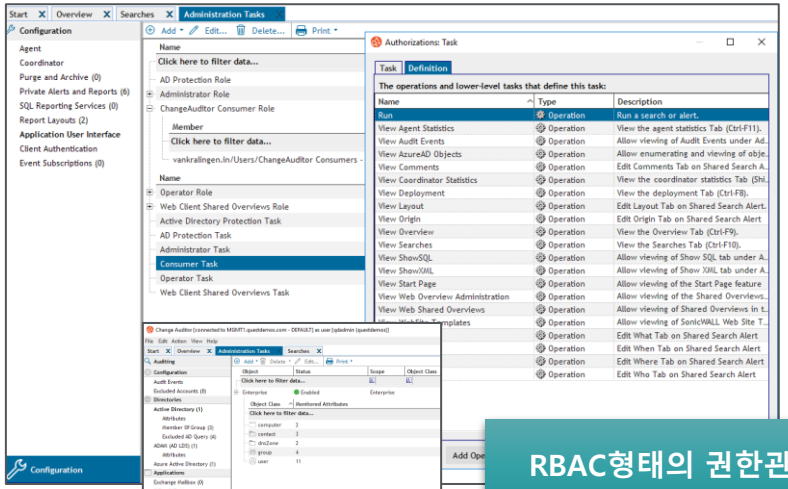


핵심 기능 – 실시간 알람 연동

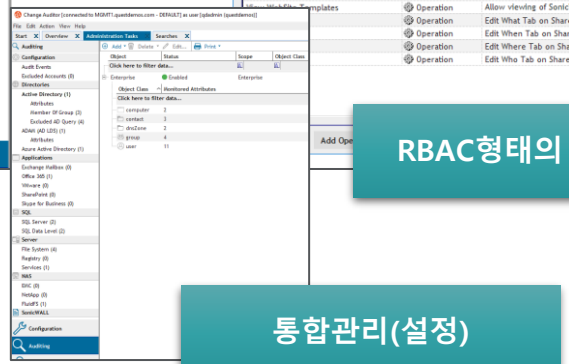


다양한 형태의 알람 연동

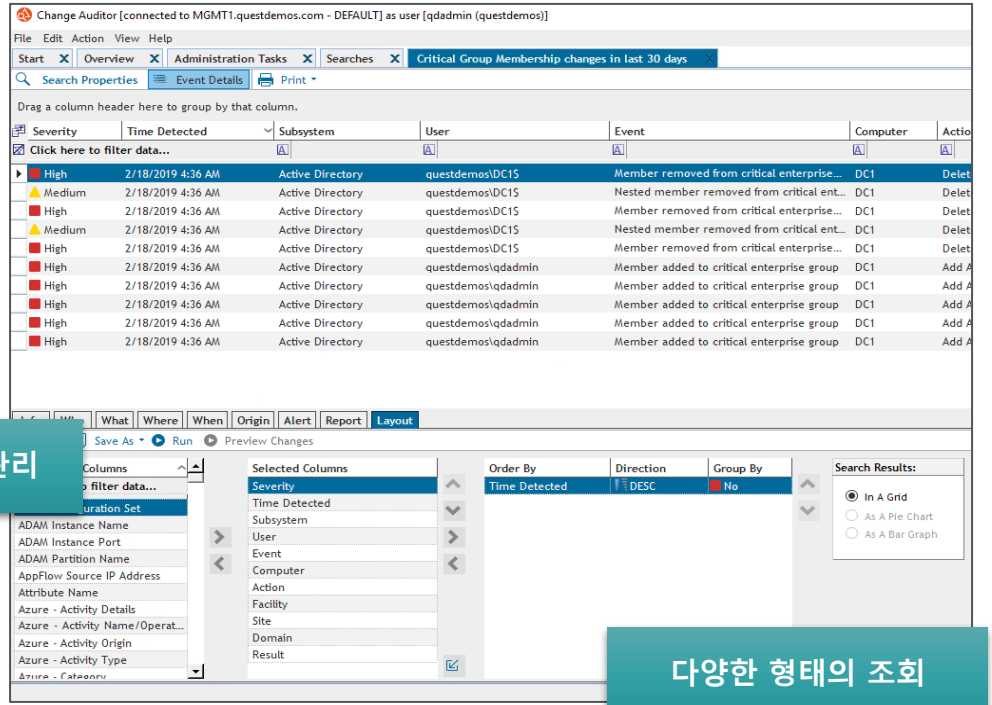
핵심 기능 – 분석 플랫폼 제공



RBAC형태의 권한관리

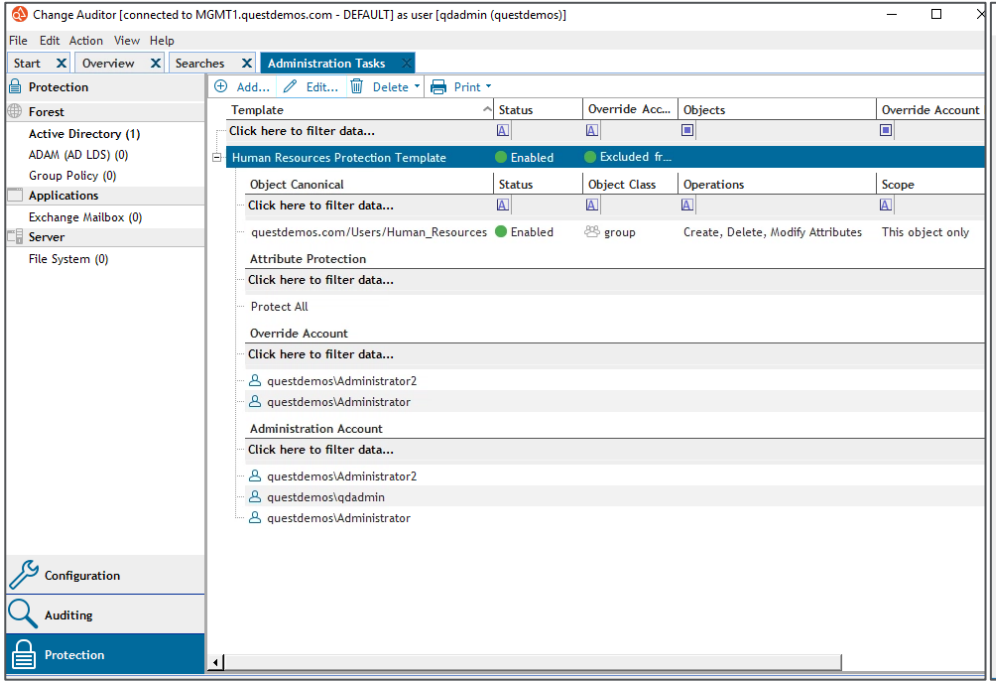


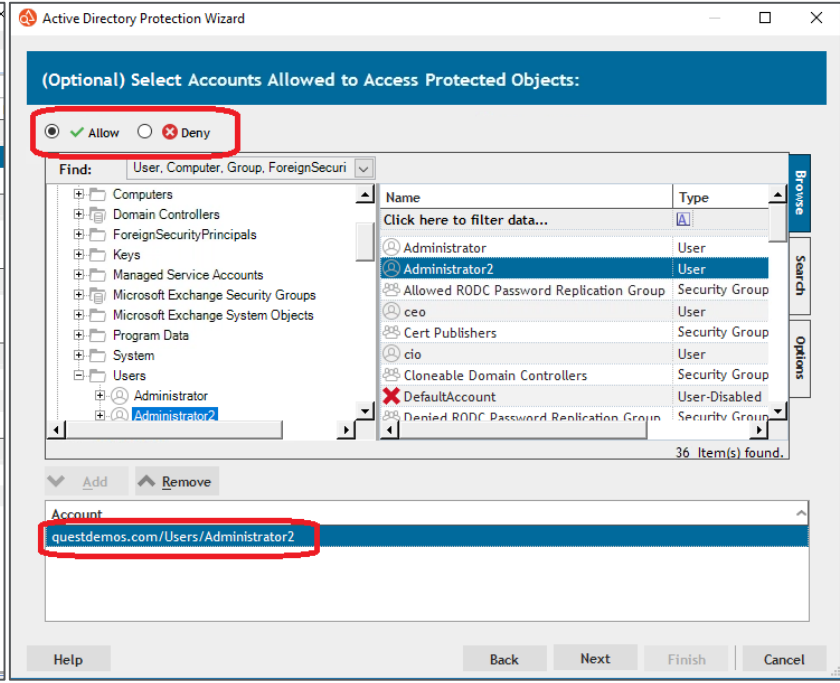
통합관리(설정)



다양한 형태의 조회

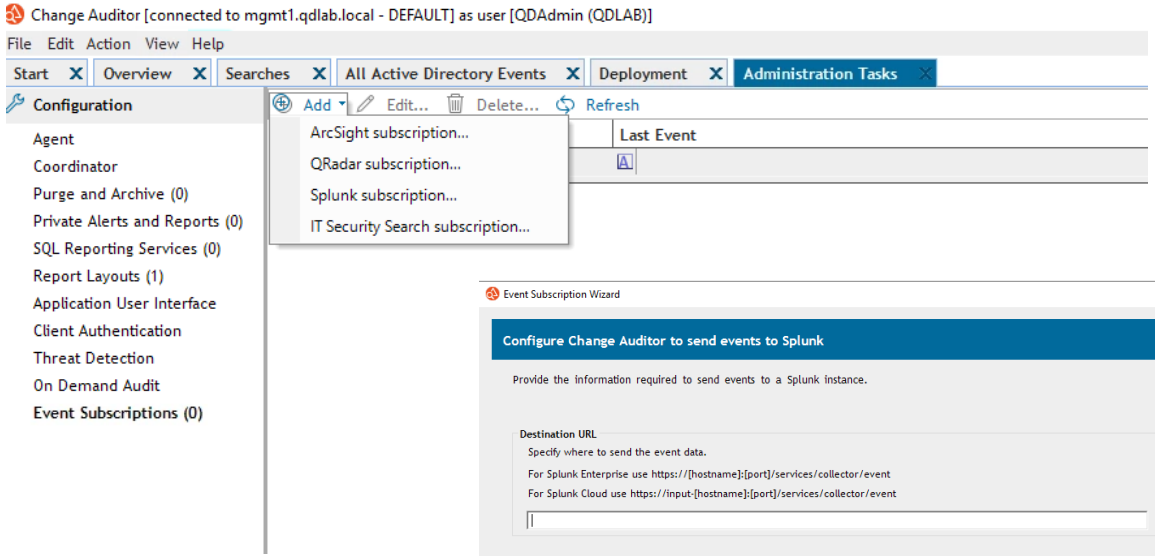
핵심 기능 – 보호기능





Where Next Meets Now.

핵심 기능 – SIEM연동



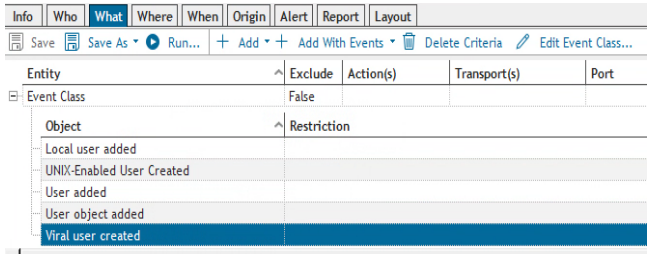
일반적인 Syslog형태의 연결도 지원

주요 활용 #1. 정책기반 위협 감시

운영과정에서 실수나 / 관리문제로 인하여 발생하는 보안 이슈

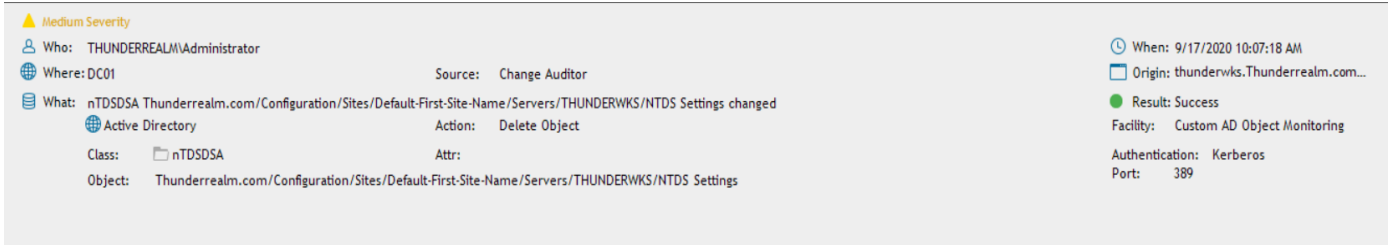
내부자나 외부 인력에 위한 위협 감시

정상적인 행위처럼 수행되는 내역에 대해서도 감사

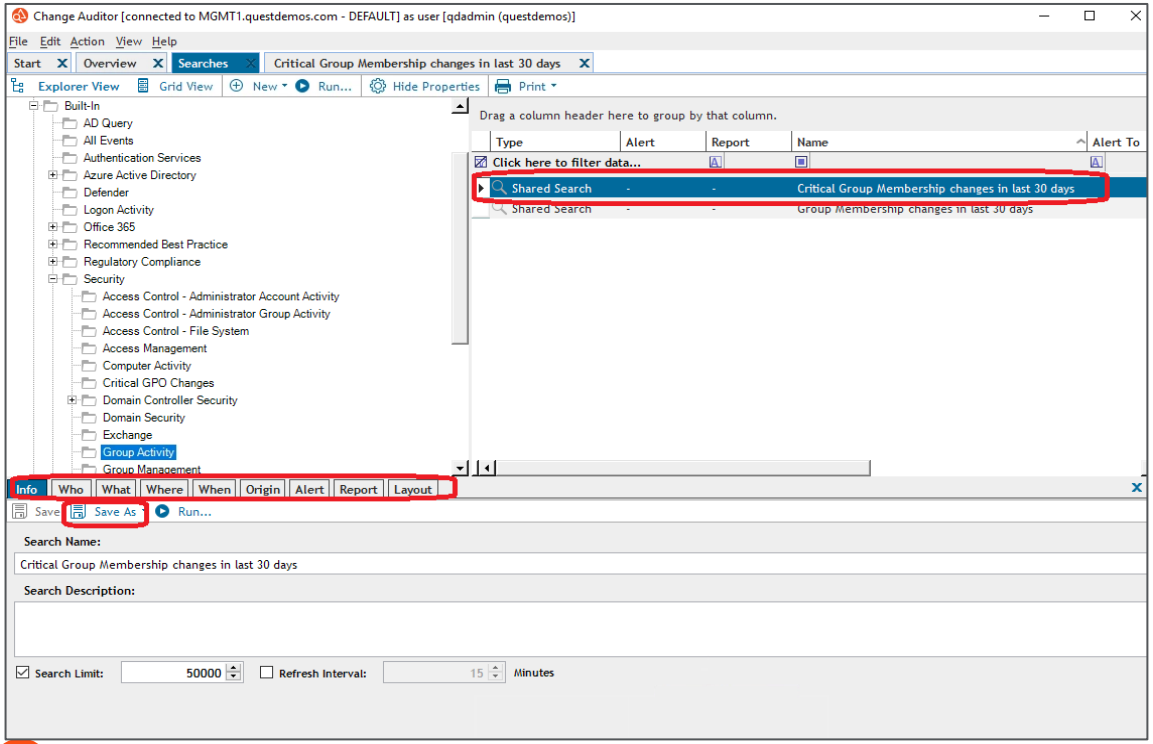


주요활용 #2. 알려진 위협 감시

알려진 위협에 대한 감시



주요 활용 #3. 분석 체계 마련 및 가시성 확보

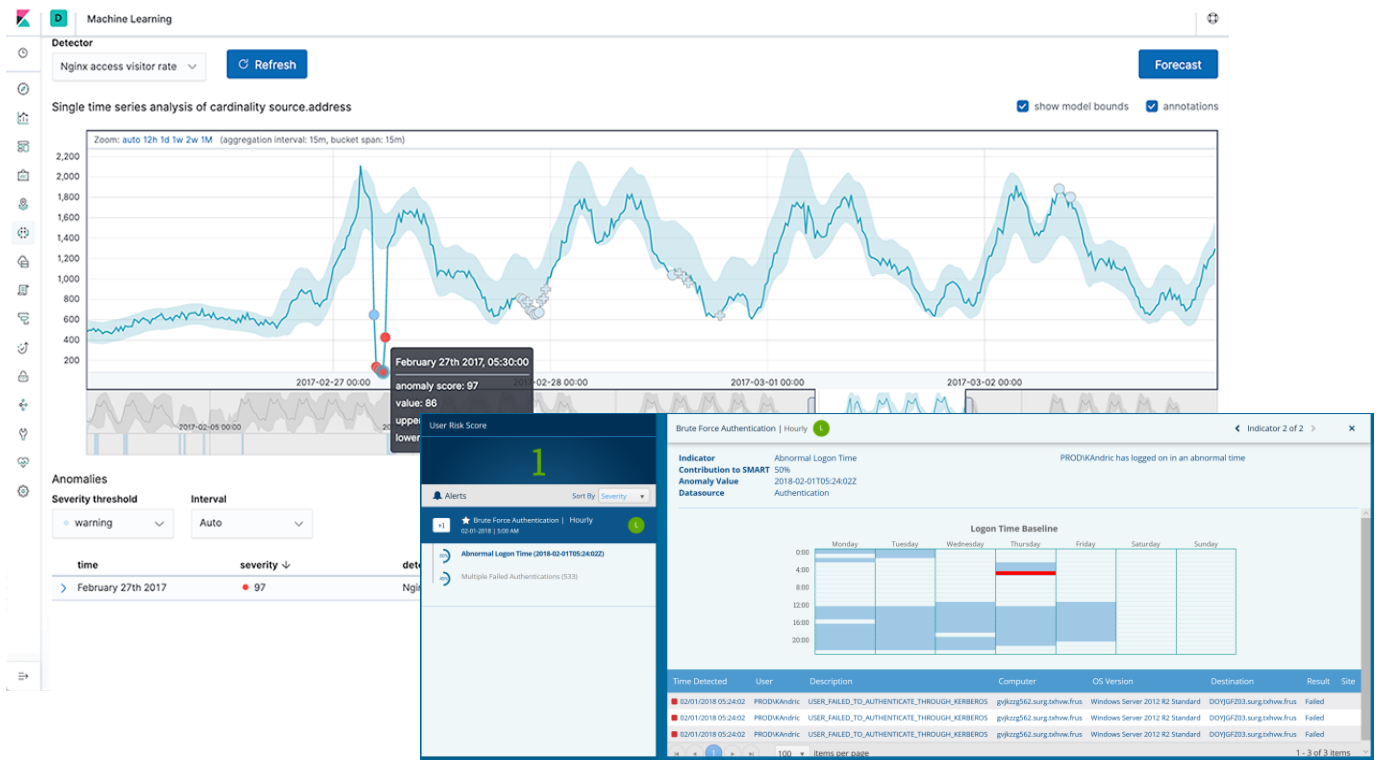


모든 데이터의 DB화 및 확장된 검색을 통한 분석 체계 제공

정의된 리포트를 통해서 원하는 데이터를 손쉽게 조회

주요 활용 #4. SIEM연동을 통한 데이터분석

데이터 전처리 형태로 SIEM에 필요한 데이터를 제공



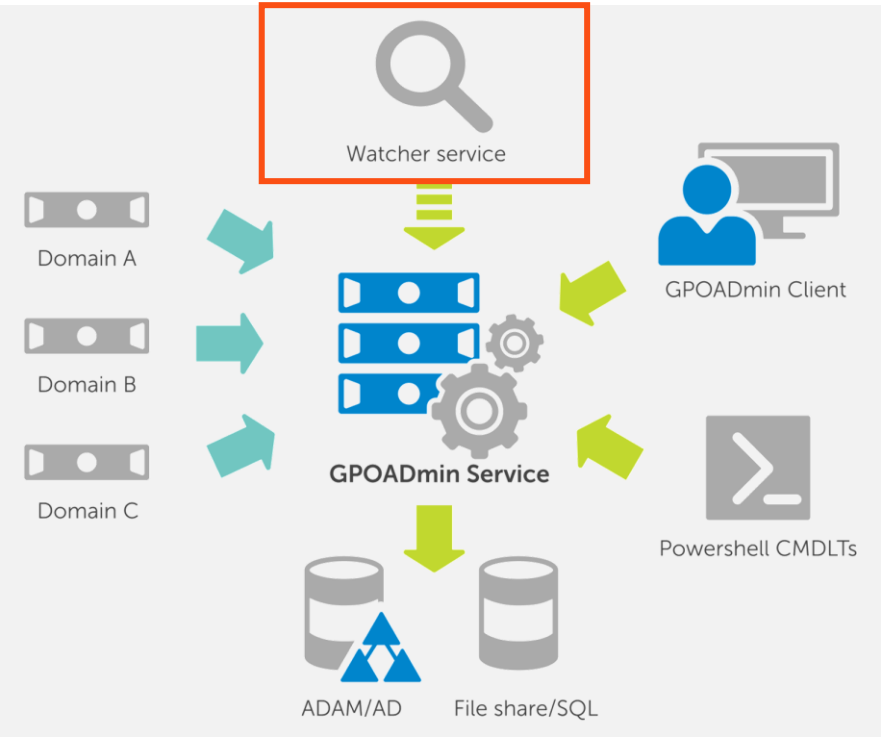
GPO 통합관리 및 접근통제

- GPOAdmin

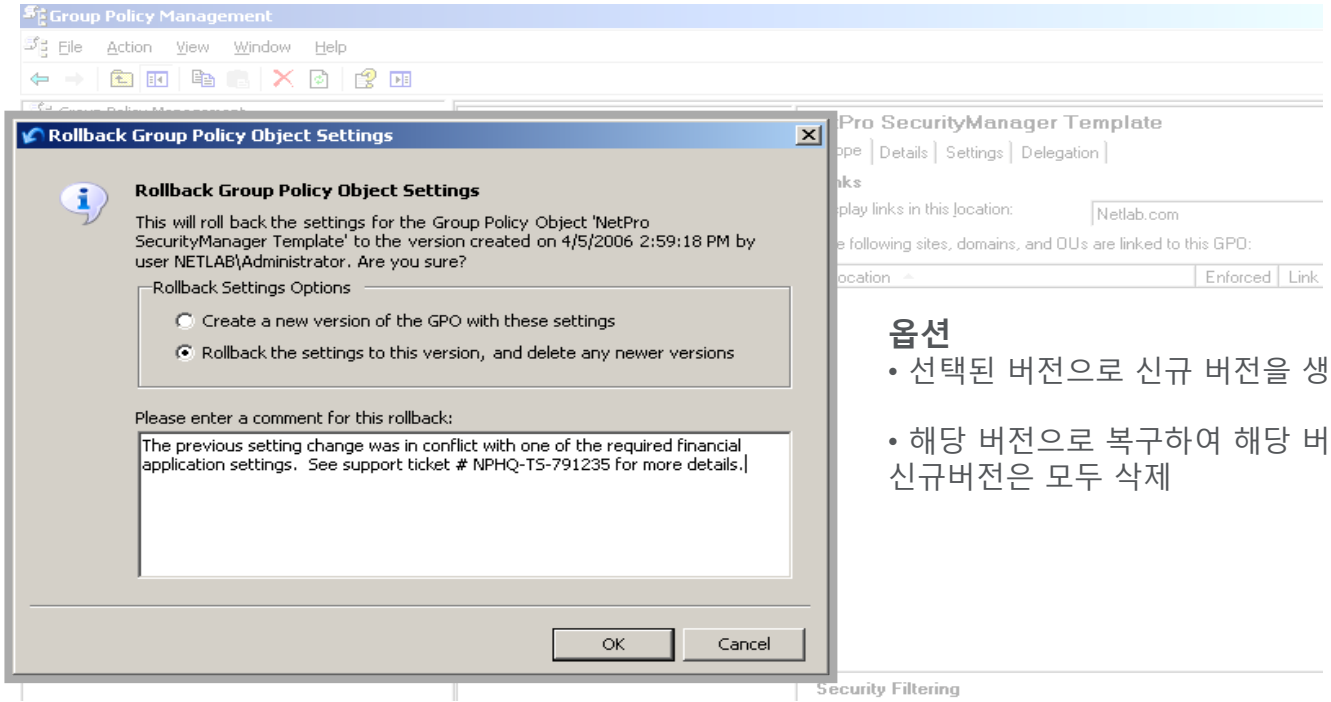
Quest

Where Next Meets Now.

핵심 기능 – Watcher를 통한 이상 생성 감시



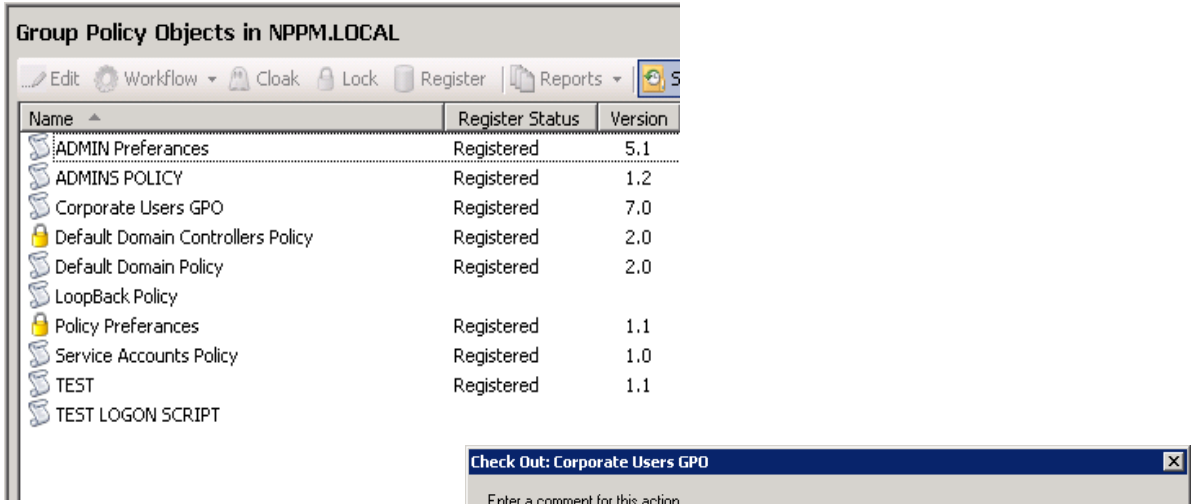
핵심 기능 – GPO 즉시 복구

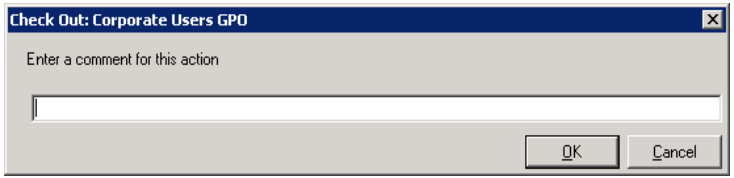


옵션

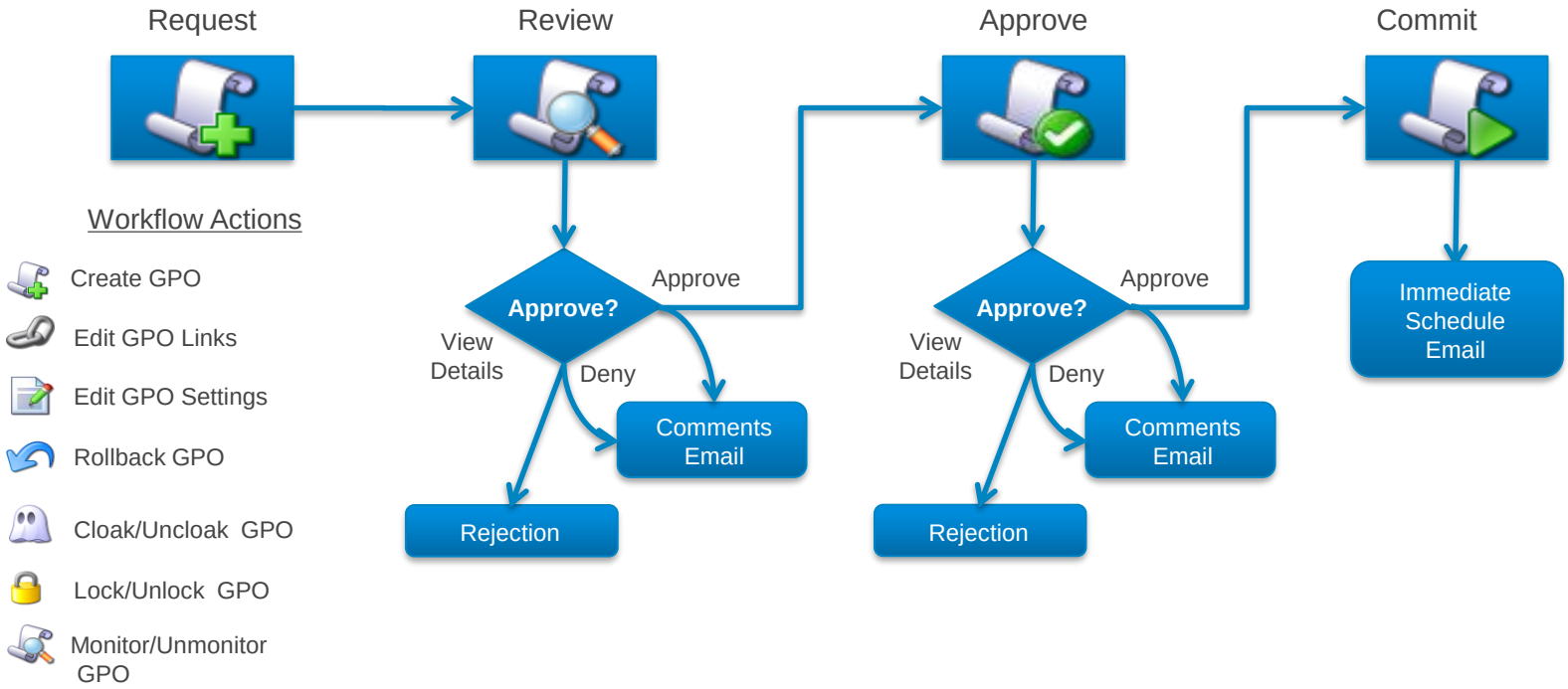
- 선택된 버전으로 신규 버전을 생성
- 해당 버전으로 복구하여 해당 버전이후 신규버전은 모두 삭제

핵심 기능 – 자동 버전 관리

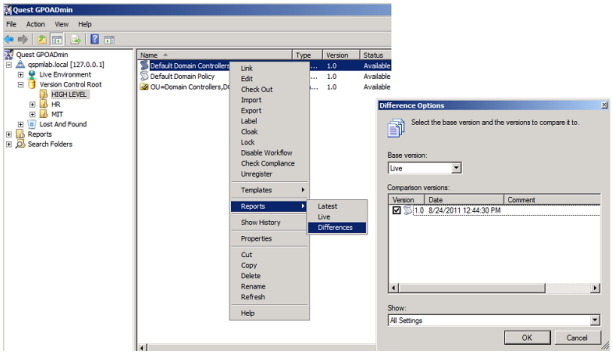


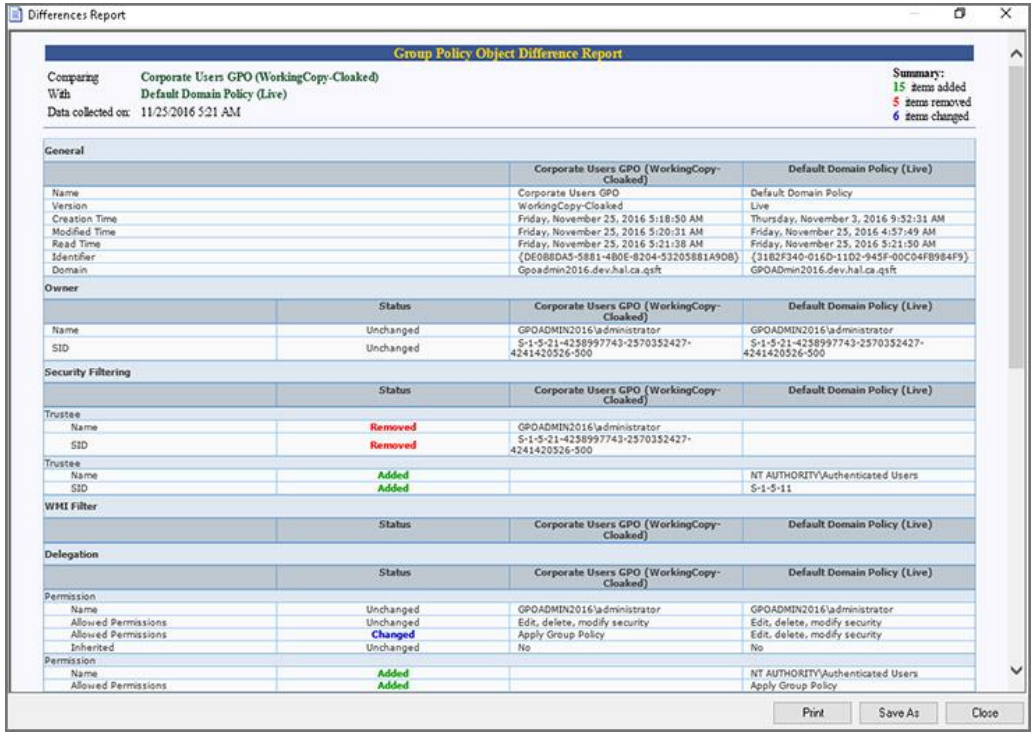


핵심 기능 – 승인기반 Workflow

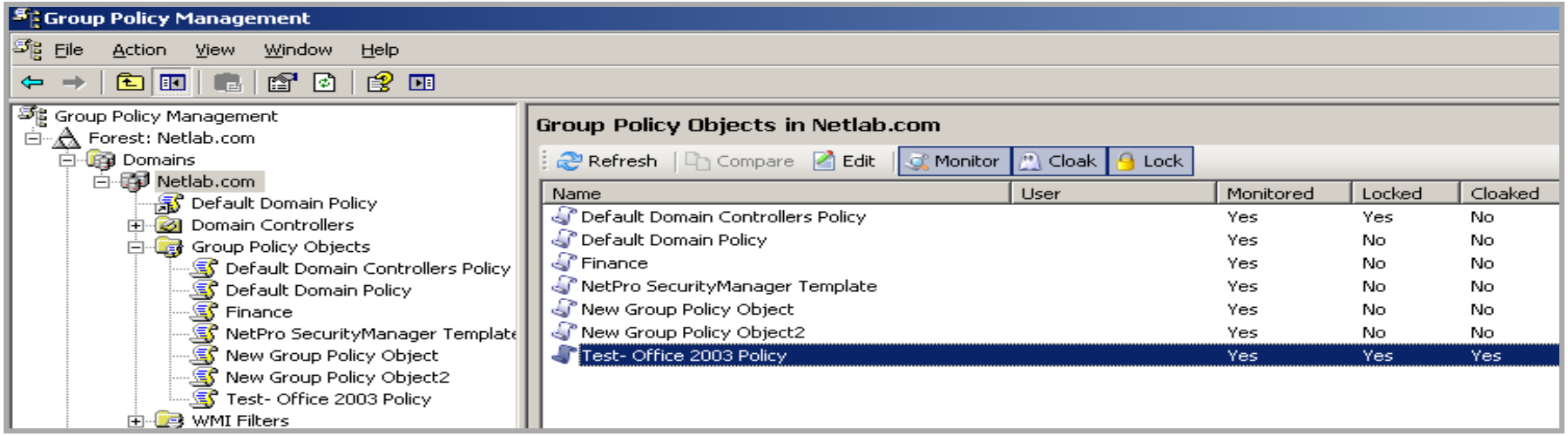


핵심 기능 – 버전별 자동 비교





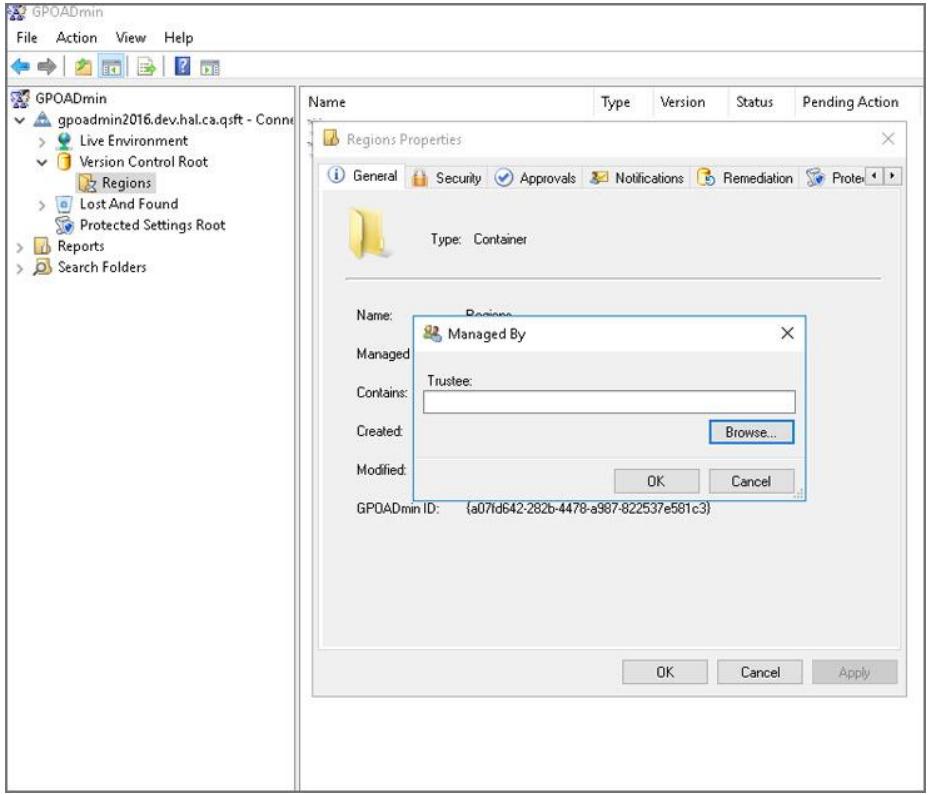
핵심 기능 – GPO 숨김 및 보호

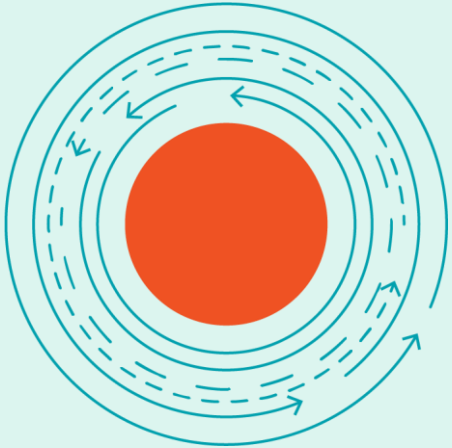


핵심 기능 – GPO별 담당자 지정

최소권한 관리를 통한 보안 향상

관리 효율성 재고





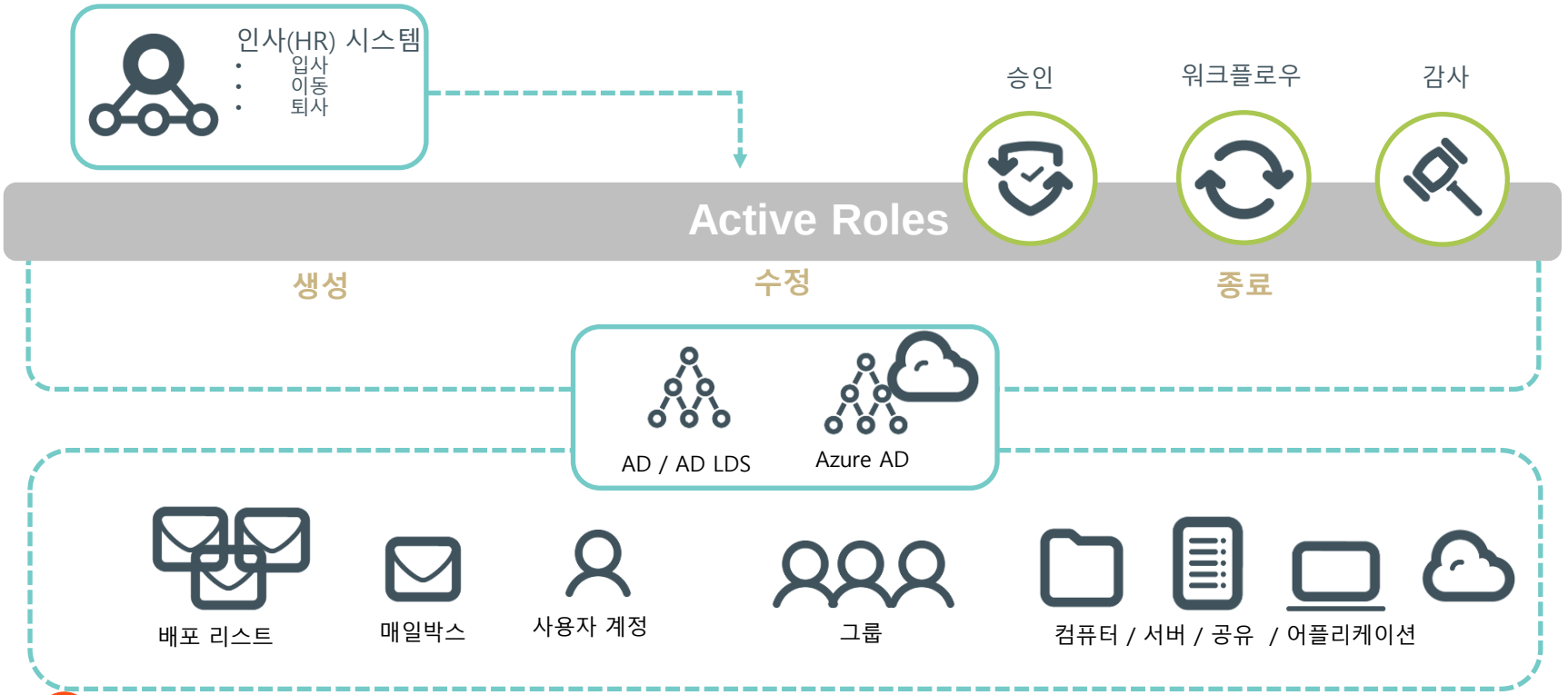
계정 접근통제 및 통합관리

- Active Roles

Quest

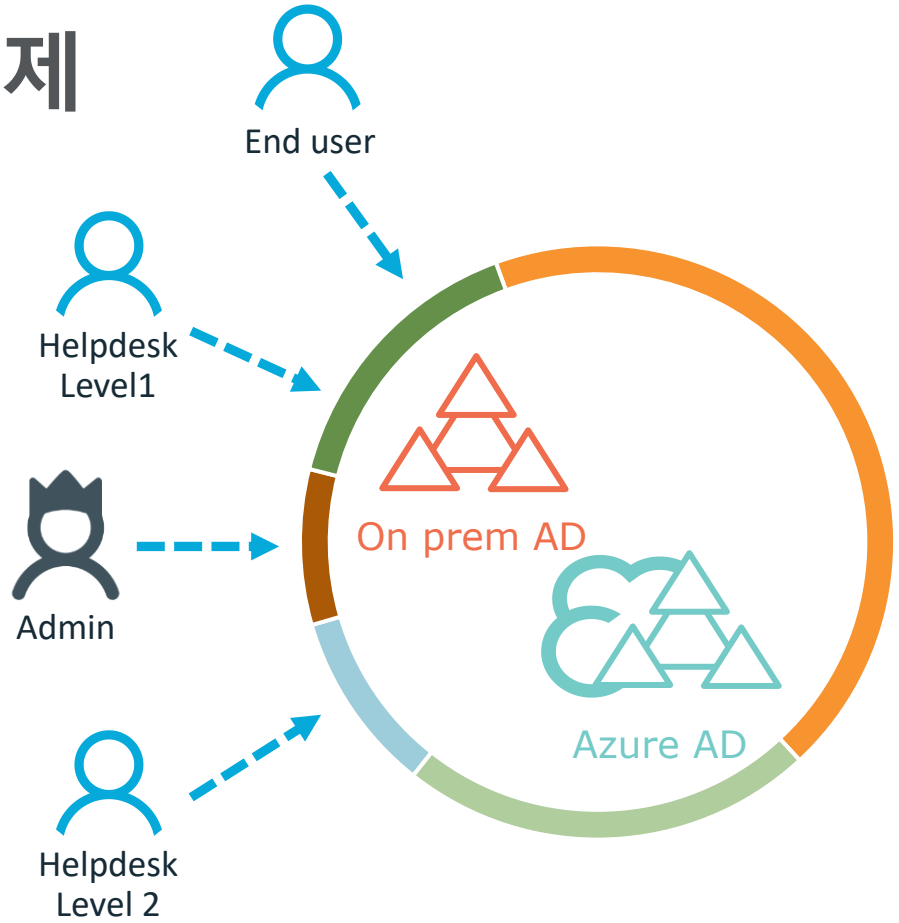
Where Next Meets Now.

AD 통합 관리


인사(HR) 시스템
• 입사
• 이동
• 퇴사
승인
워크플로우
감사
Active Roles
생성
수정
종료
AD / AD LDS
Azure AD
배포 리스트
매일박스
사용자 계정
그룹
컴퓨터 / 서버 / 공유 / 어플리케이션

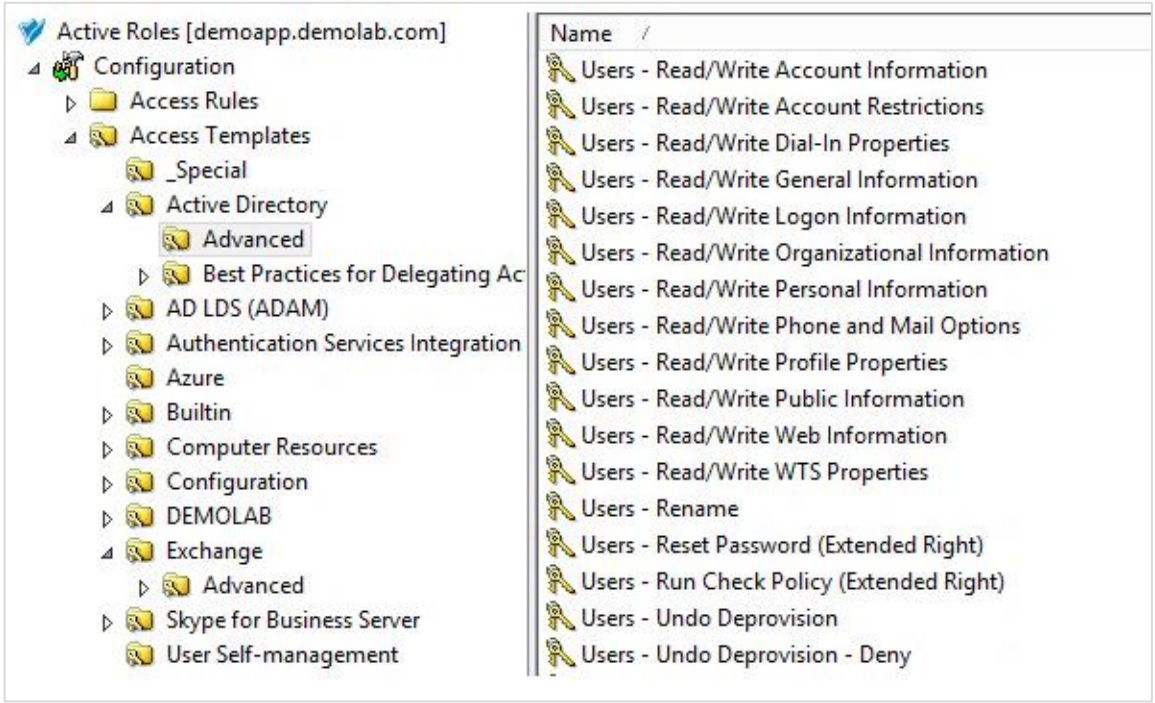
핵심 기능 - AD 접근통제

- 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

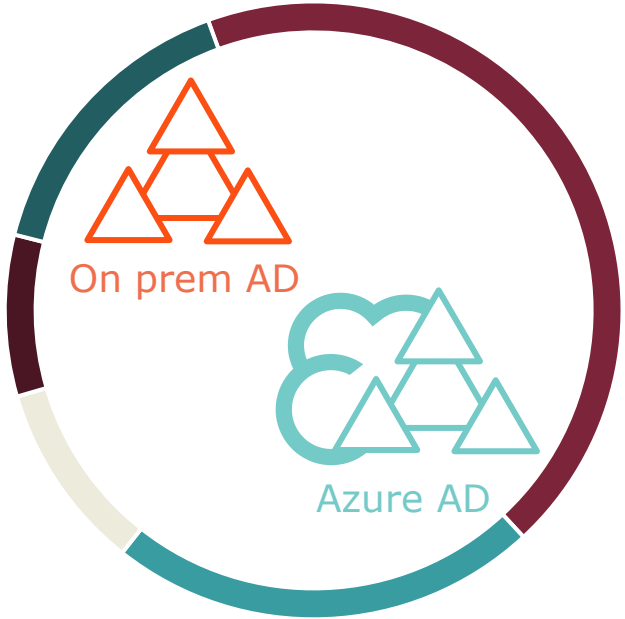


핵심 기능 - 완벽한 사용자 라이프사이클 관리

인사(HR)시스템
- 입사
- 이동
- 퇴사

Active Roles

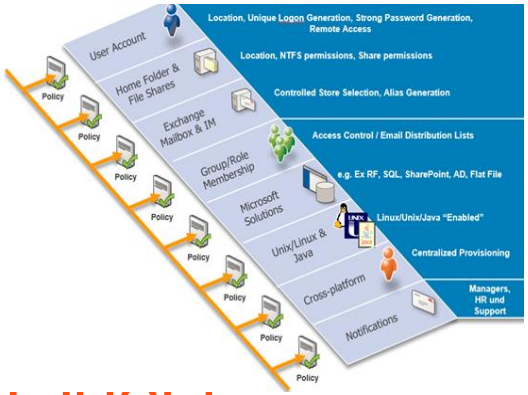
완벽한 사용자 라이프사이클 관리



O365와 Cloud기반 SaaS서비스도 지원

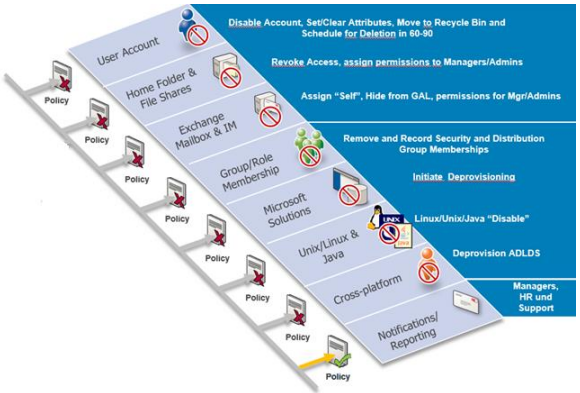
프로비저닝

외부 계정 자동 생성



디-프로비저닝

외부 계정 자동 제거



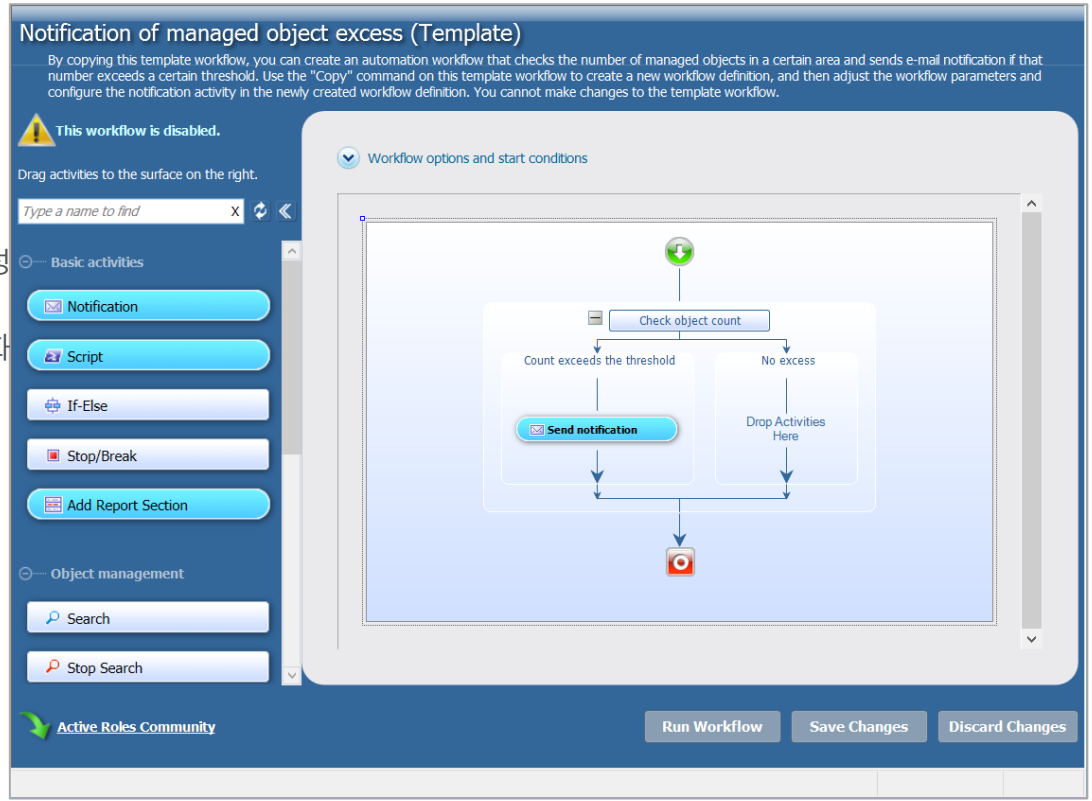
핵심 기능 - 워크플로우 엔진

- **사용자 정의 자동화된 워크플로우**

- 작업에 대한 요청을 승인처리

- GUI기반의 워크플로우 엔진 제공을 통한 손쉽게 생성

- 워크플로우 기반의 관리를 통해서 프로세스의 자동화

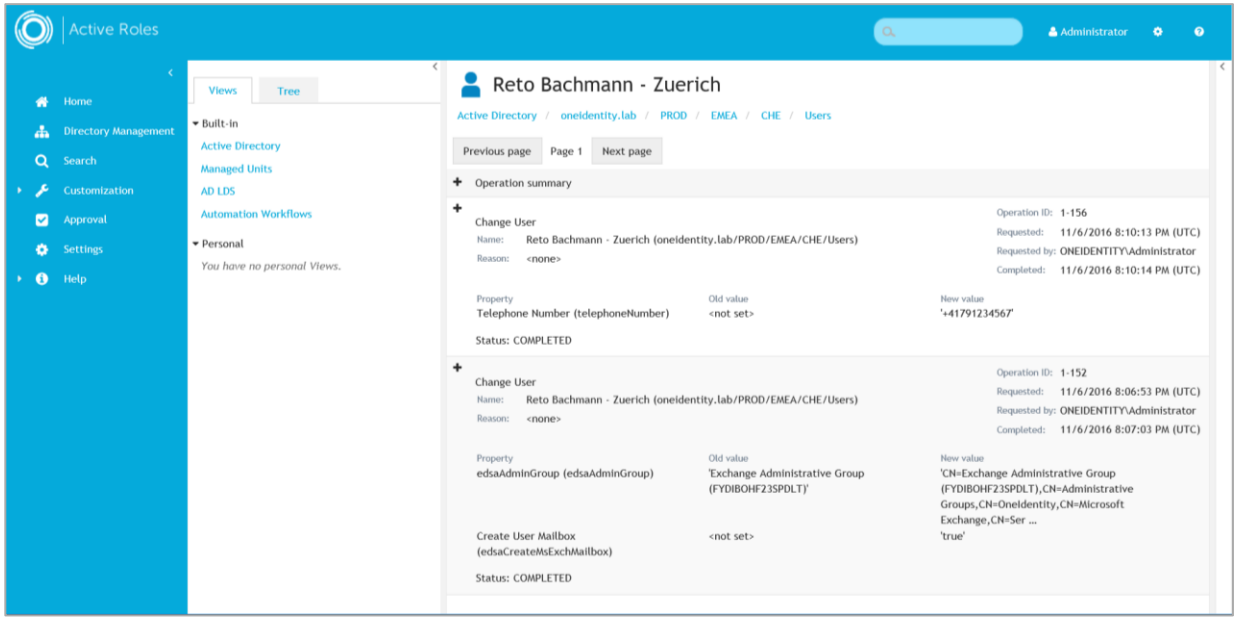


핵심기능 - 모든 변경 내역을 제공

- **Active Roles내에서 발생한 모든 변경 기록 정보를 제공**

모든 변경 기록정보 제공으로 자체적인

보안감사 및 이슈 분석 가능




Thank You
Quest
Where Next Meets Now.