

하이브리드 AD환경에서의 침해 진단, 탐지부터 복구까지 한번에 이해하기

Solution Consultant / Hongso Chae

Active Directory Keystone

Active Directory는 **Keystone**

Active Directory
인증과 접근에 핵심

Databases

SQL Server, Oracle, MySQL,
Postgres + 등

Files

서버나 클라우드 저장되는
파일과 디렉토리

Applications

Office 365, Teams,
SharePoint, Exchange,
Cloud Apps (SaaS),
Bespoke apps

Endpoints

사용자들이 접근하는
노트북, 서버

95M 개의 Active Directory
계정이 매일 공격을
받고 **1.2M개의** Entra ID
계정이 매달 손상을 입음

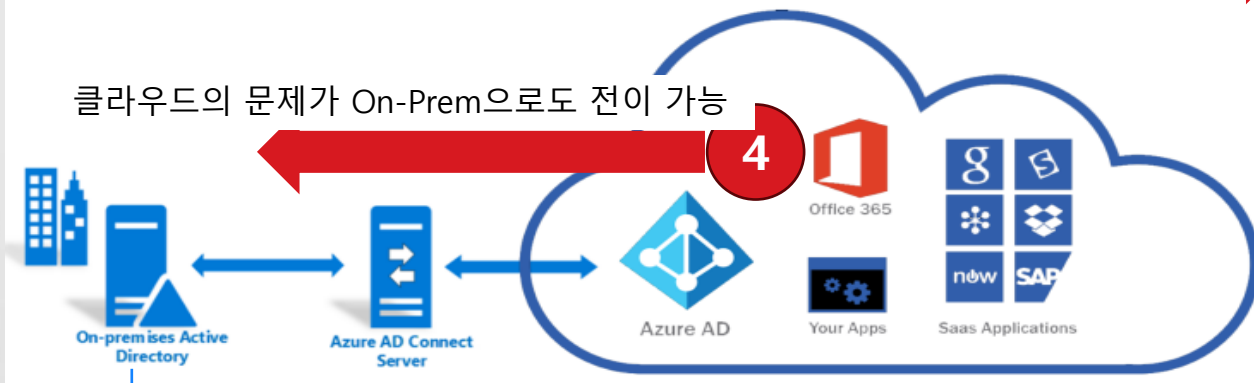
하이브리드 환경은 높은 보안과 빠른 복구를 필요

Hybrid AD 환경의 이해

1



공격 표면과 보안 위협의 확대



인터넷을 통해서 접근할 수 있는 접근성이 추가

3

계정과 데이터는 고객 관리 영역

2



- On-Prem AD의 보안 이슈가 그대로 전이
- On-Prem의 이상 데이터 변경이 그대로 적용



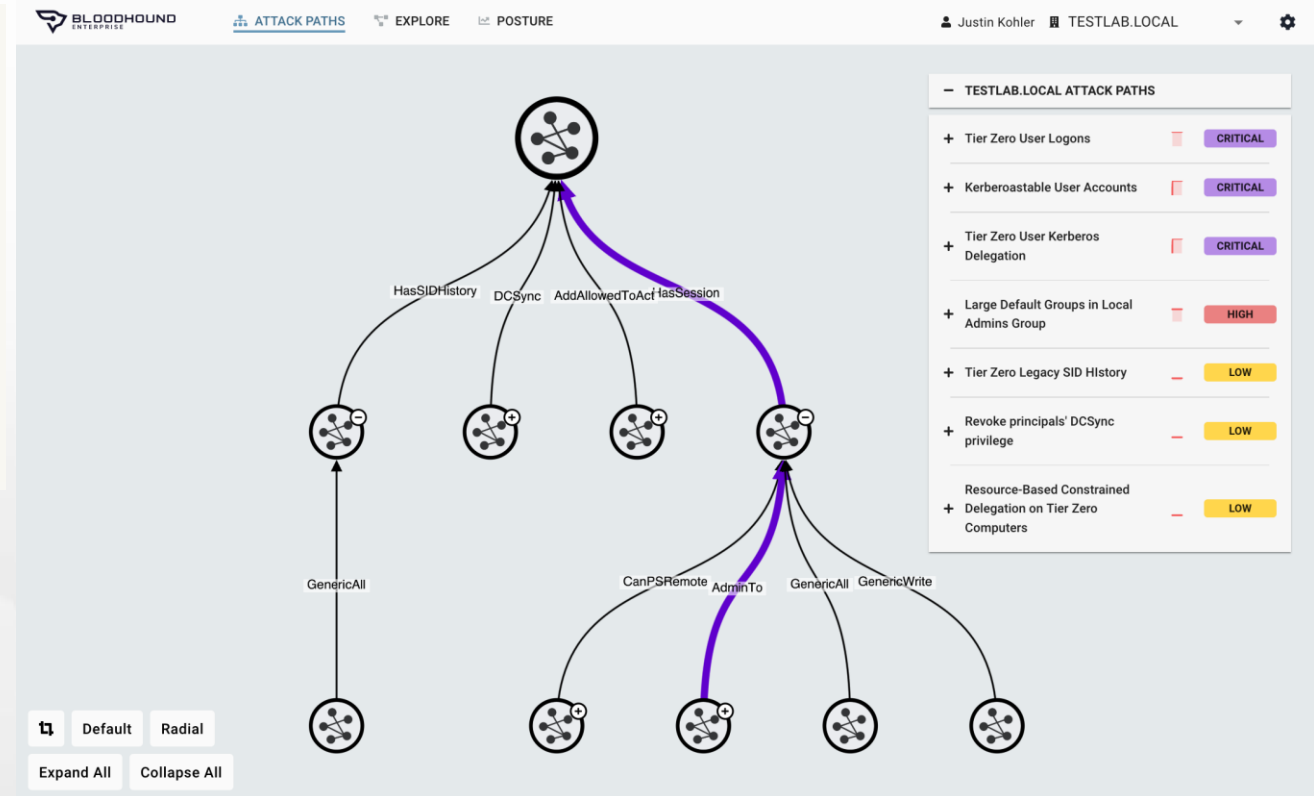
Responsibility		SaaS	PaaS	IaaS	On-prem
Responsibility always retained by the customer	Information and data	Customer	Customer	Customer	Customer
	Devices (Mobile and PCs)	Customer	Customer	Customer	Customer
Responsibility varies by type	Accounts and identities	Customer	Customer	Customer	Customer
	Identity and directory infrastructure	Shared	Customer	Customer	Customer
	Applications	Customer	Customer	Customer	Customer
	Network controls	Customer	Customer	Customer	Customer
Responsibility transfers to cloud provider	Operating system	Microsoft	Microsoft	Microsoft	Customer
	Physical hosts	Microsoft	Microsoft	Microsoft	Customer
	Physical network	Microsoft	Microsoft	Microsoft	Customer
	Physical datacenter	Microsoft	Microsoft	Microsoft	Customer

Legend: Microsoft (light blue), Customer (dark blue), Shared (diagonal split)

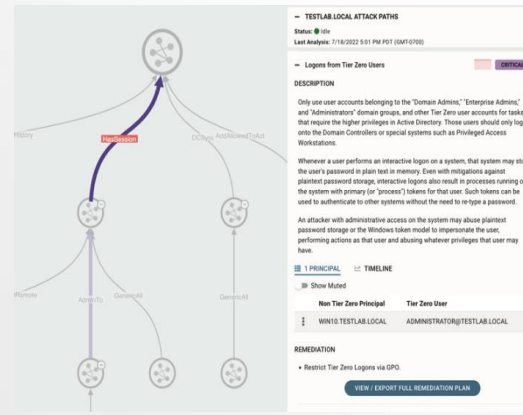
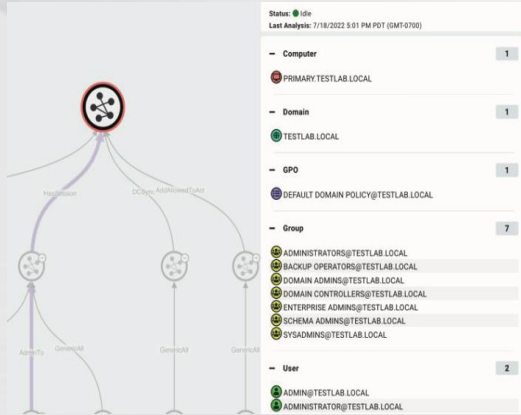
전략1. 공격표면 관리 (사전 위협 제거)

핵심은 Attack Path

보안 위협의 핵심은 계정탈취 -> 계정탈취를 위한 공격 경로



공격경로 분석 및 제거



Add Secret to Tier Zero Service Principal or App

Recommended Remediation

Remediation of this finding will depend on whether the non Tier Zero principal has been granted a tenant-scoped, service principal-scoped, or app-scoped role assignment. Additionally, this finding may be produced when the non Tier Zero principal has been granted explicit ownership of the service principal or app.

Removing Tenant-scoped role assignment:

- Using a Tier Zero user account, log into the Azure portal at <https://portal.azure.com>.
- Search for or click on "Azure Active Directory".

Description

Azure provides several systems and mechanisms for granting control of securable objects within Azure Active Directory, including tenant-scoped admin roles, object-scoped admin roles, explicit object ownership, and API permissions.

When a principal has been granted "Cloud App Admin" or "App Admin" against the tenant, that principal gains the ability to add new secrets to all Service Principals and App Registrations. Additionally, a principal that has been granted "Cloud App Admin" or "App Admin" against, or explicit ownership of a Service Principal or App Registration gains the ability to add secrets to that particular object.

References

MITRE ATTACK

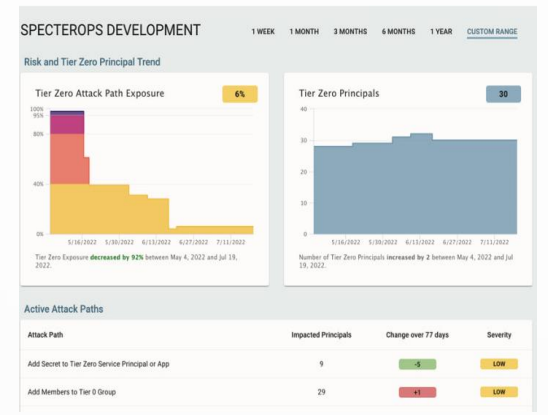
- ATTACK T1098: Account Manipulation

How Attackers Abuse This Attack Path

- Andy Robbins - Azure Privilege Escalation via Service Principal Abuse

Microsoft Reference Documentation

- Assign Azure AD roles at different scopes



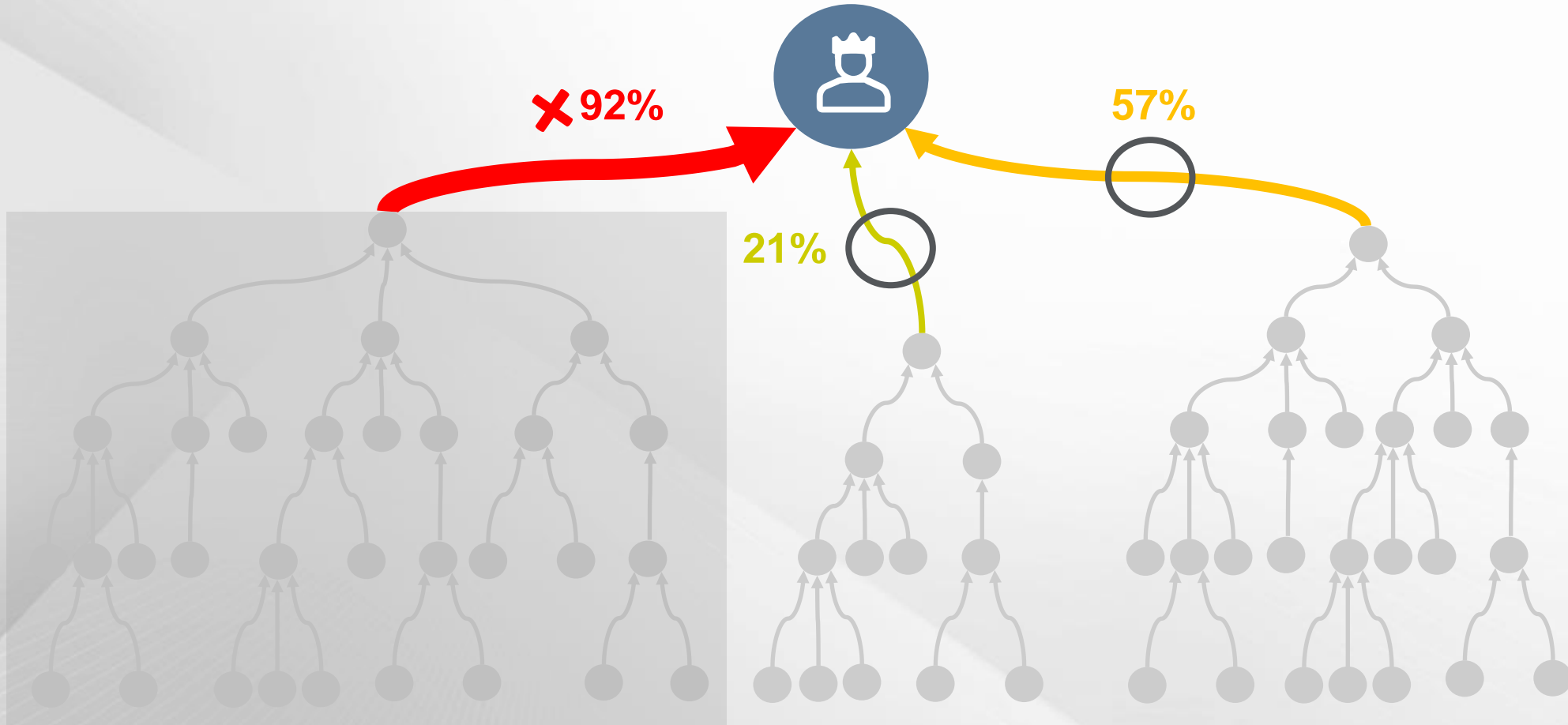
지속적인 Attack Path 분석

Attack Path의 주요경로 분석 (핵심 구간 분석)

문제 해결을 위한 가이드 제공

주요한 위협 지표 제공

공격경로 분석 및 제거



하나의 개선으로 수만은
Attack Path를 제거

상세 가이드 제공

BLOODHOUND ENTERPRISE ATTACK PATHS EXPLORE POSTURE Justin Kohler TESTLAB.LOCAL


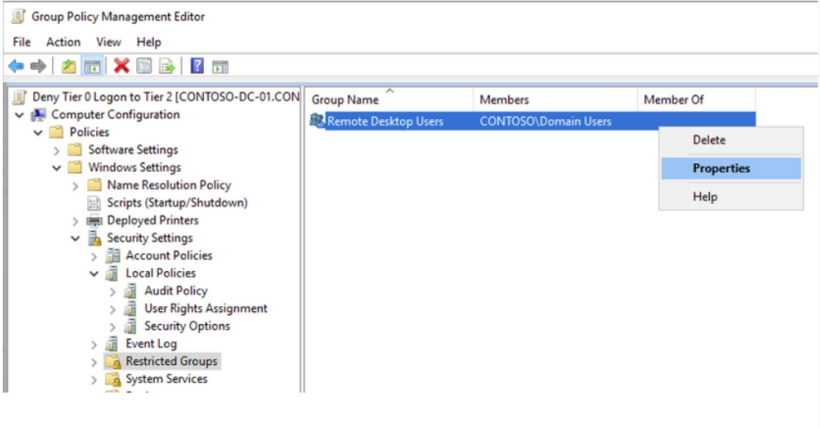
Recommended Remediation

Remove groups which grant an excessive number of users execution and local admin rights to any system from the local admins, Remote Desktop Users, Distributed COM, and Remote Management local groups on each system.

If Group Memberships are Controlled by Group

- Determine which GPOs are applied to the machine and typing the following command:

```
C:\> gpresult /v /scope computer
```
- Inspect each GPO in GPEdit to determine which policies are controlling local groups. The specific policy is located at:
Computer Configuration / Policies / Windows Settings / Security Settings / Restricted Groups
- Right click on the local group, then click properties.
- Under Members of this Group, click the group, then click Remove. Repeat this for all groups containing large amounts of users.



Large Default Groups in Local Admins Group

Description

Group delegated privilege should be tightly controlled to only grant remote command execution and local administration privileges to authorized principals.

Technical Background

The Windows operating system grants remote execution privilege to principals that belong to the Local Administrators, Remote Desktop Users, Distributed COM Users, and Remote Management Users groups. Additionally, Windows grants remote execution privilege to principals that belong to Active Directory security groups that have been added to the aforementioned local groups.

Three default groups within Active Directory (DOMAIN USERS, AUTHENTICATED USERS, EVERYONE) should arguably never be members of local groups on any machine as this is against best practice for least privilege. When an adversary discovers a system where most or all domain authenticated users have remote execution and/or admin rights, such systems can provide the attacker with their first step in a critical attack path leading to the compromise of the entire enterprise.

References

- CWE-250: Execution with Unnecessary Privileges

EXPORT (.ZIP)

전략2. 위협 보호 및 탐지

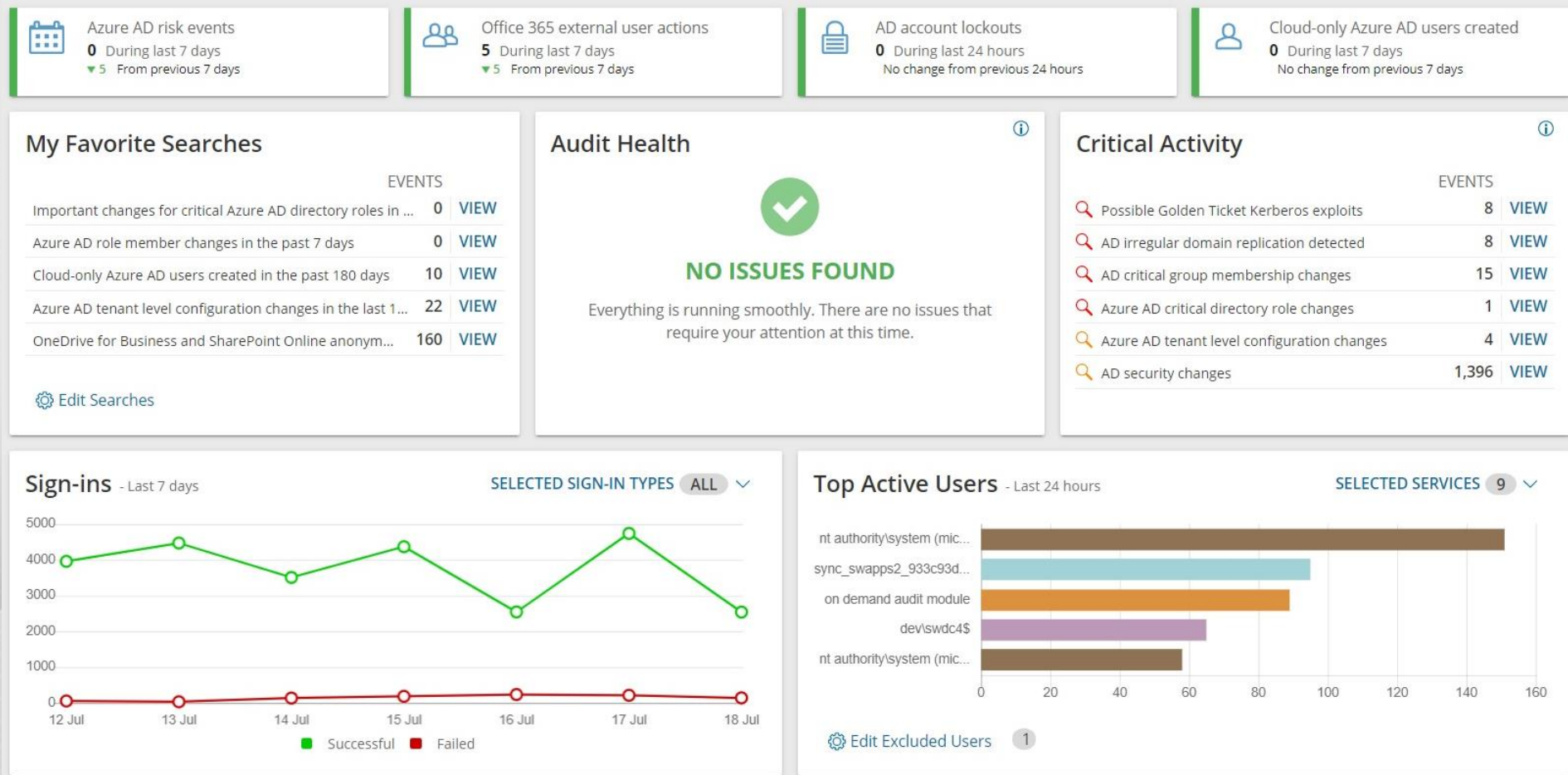
Hybrid환경의 모든 이벤트를 통합

- 단일뷰 로 Hybrid 환경과 M365환경을 지원
- SaaS방식의 서비스 제공



통합 위협 대시보드 제공

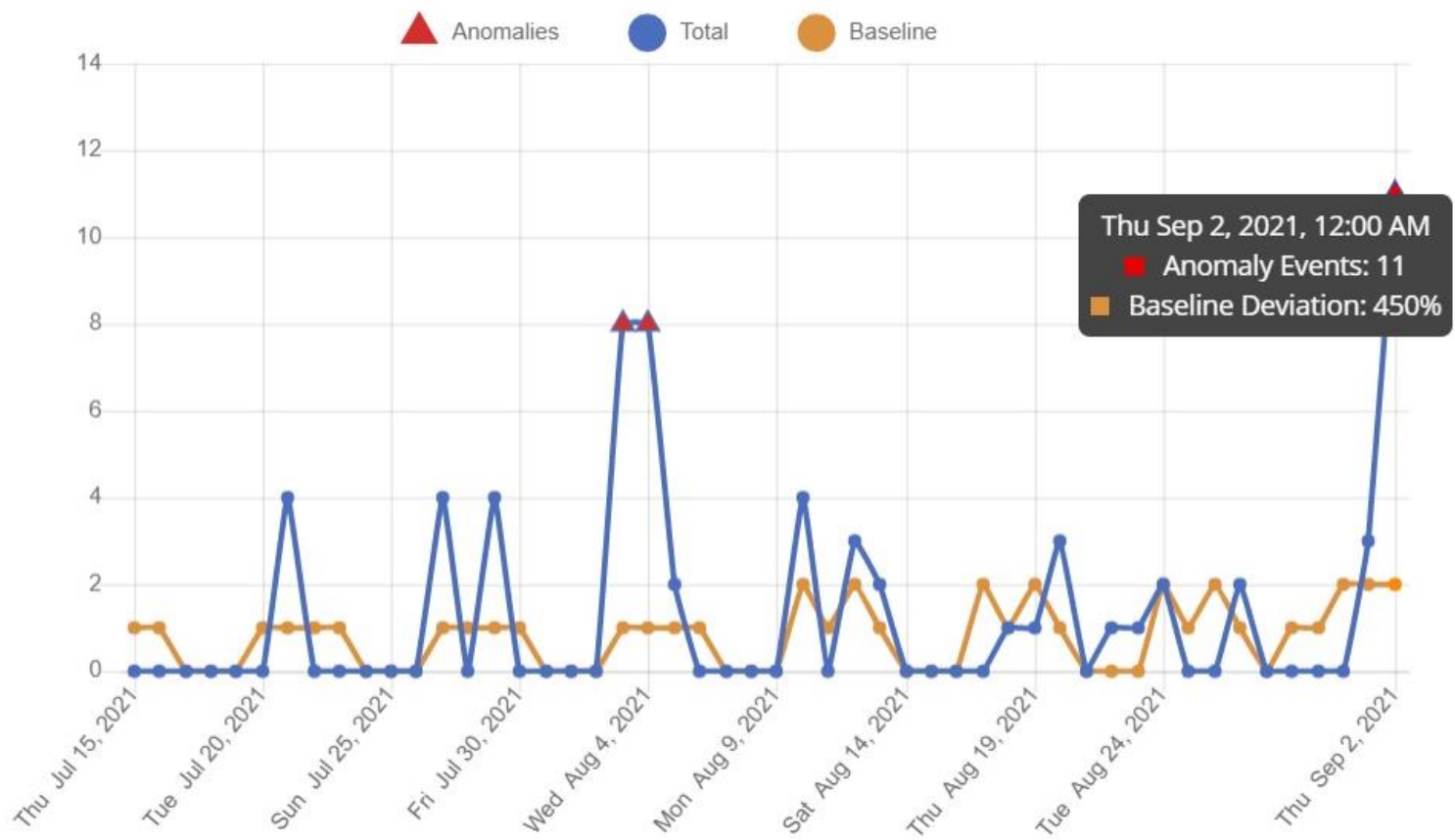
- Proactively analyze on-prem and cloud data for key security vulnerabilities



머신러닝 기반의 위협 탐지

Unusual increase in tenant sign-in failures in the past 60 days for TitanCorp

An unusual increase in sign-in failures could suggest a user or configuration issue or possibly a password-guessing attack.



위협 보호 제공



전략3. 복구 및 DR

비용 손실

FORRESTER

The Total Economic Impact™ Of Quest Recovery Manager For Active Directory Disaster Recovery Edition

Avoided Costs, Losses, And Excess Labor By Recovering Faster With Quest Recovery Manager For Active Directory Disaster Recovery Edition

FEBRUARY 2023

A FORRESTER TOTAL ECONOMIC IMPACT™ STUDY COMMISSIONED BY QUEST

EXECUTIVE SUMMARY

- Active Directory disaster recovery **Reduced from 30 to 3 hours**
- Value of recovering with RMAD DRE following a ransomware attack **\$19.7 million**
- Object- and group-level recovery **90% faster**
- Three-year benefits (PV) **\$1.1 million**

Benefits (Three-Year)

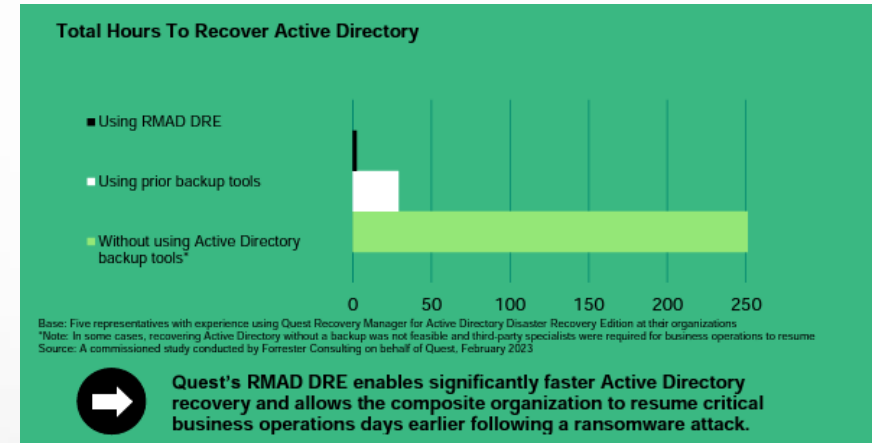
- Faster and more accurate recovery from a disaster scenario (weighted by likelihood of attack) **\$679.1K**
- Faster and more comprehensive object- and group-level recovery **\$470.3K**

Benefit calculations

“There are other backup tools out there, but they don’t do the automation or orchestration. They don’t give my business the same level of guarantee. In the end, RMAD DRE is best-of-breed.”

— Vice president of enterprise services, managed service provider

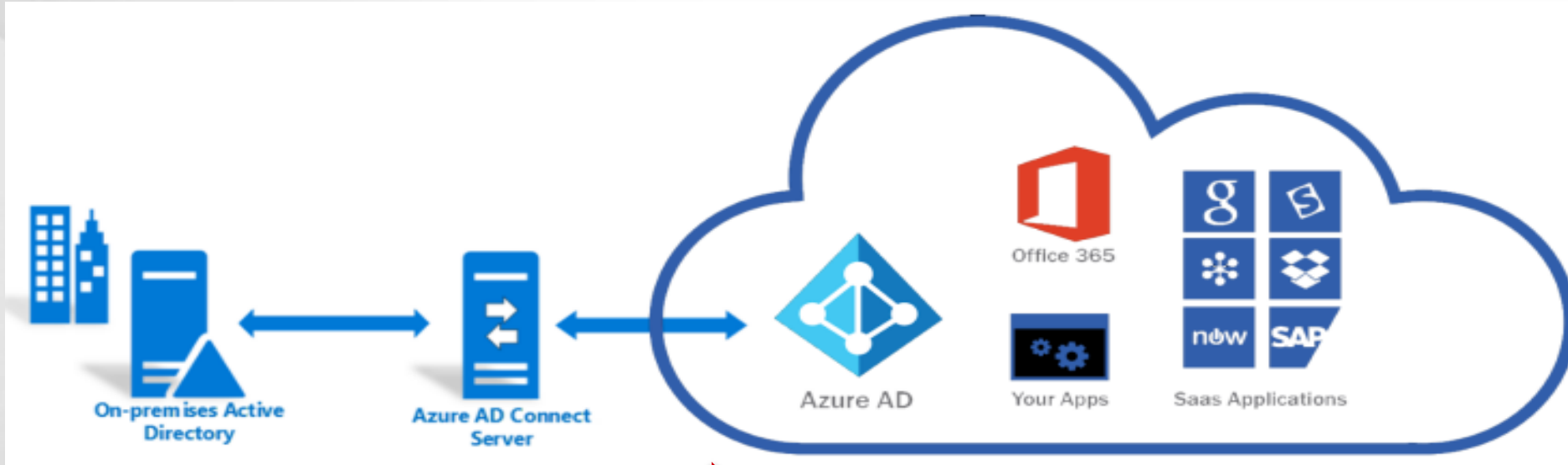
- 90%의 복구 시간 감소
- AD 다운으로 인한 비용 = 1시간당 \$730K



Faster And More Accurate Recovery From A Disaster Scenario (Weighted By Likelihood Of Attack)

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Cost of one hour of downtime during ransomware attack	Interviews	\$730,000	\$730,000	\$730,000
A2	Hours to recover Active Directory without Quest RMAD DRE	Interviews	30	30	30
A3	Business losses during Active Directory recovery	A1*A2	\$21,900,000	\$21,900,000	\$21,900,000
A4	Reduction in time to recover Active Directory due to Quest RMAD DRE	Interviews	85%	88%	90%
A5	Hours to recover Active Directory with Quest RMAD DRE	A2*(1-A4)	4.5	3.6	3.0
A6	Business value protected due to Quest RMAD DRE during the event of a ransomware attack	A3*A4	\$18,615,000	\$19,272,000	\$19,710,000
A7	Average likelihood of a successful ransomware attack impacting Active Directory each year	Ponemon	1.5%	1.5%	1.5%
A8	Faster and more accurate recovery from a disaster scenario (weighted by likelihood of attack)	A6*A7	\$279,225	\$289,080	\$295,650
	Risk adjustment	15%			
Atr	Faster and more accurate recovery from a disaster scenario (weighted by likelihood of attack) (risk-adjusted)		\$265,264	\$274,626	\$280,868
Three-year total: \$820,757			Three-year present value: \$679,132		

복구 및 DR 체계 필요성



AD 데이터이슈가 O365로 확대

O365 자체 데이터 손실

- ✓ Office 365 licenses
- ✓ Mailbox
- ✓ Application role assignments
- ✓ Office 365 groups & Teams membership
- ✓ Multi-factor authentication & password reset configuration
- ✓ Azure AD Roles membership
- ✓ Conditional Access Policies rules
- ✓ Custom properties for cloud applications
- ✓ SharePoint permissions

AD 자체 DR 및 데이터 손실 > 서비스 중단으로 인한 비즈니스 연속성

AD 복구에서의 주요한 Challenges

복구 시나리오가 준비되어 있는가?

복구에 얼마나 많은 시간이 필요한가?

Trust, 데이터 Validation 등의 문제에 대해서 대응 가능한가?

복구를 위한 전문 지식이나 경험?

- 솔루션 내에서 시나리오별 Project 생성 및 주기적인 Project 검증 가능
- Forest Level의 복구 시나리오 지원
- DR 체계가 마련되어 있는가?

다양한 복구 옵션을 통하여 일반 환경에서 1시간내외 복구를 지원

데이터 복구 뿐만 아니라 Trust와 관련된 Password의 자동 Reset 지원

자동화된 복구 지원 으로 전문 지식없이 손쉽게 복구 가능

1. Forest Level의 Project 관리

Active Directory forest: rmad.local DCs to be processed: 3 of 3 Domains to be processed: 2 of 2
Pending DCs: 0 Succeeded DCs: 3 Failed DCs: 0
Elapsed time: 00:00:27

Computer	Type	Recovery Method	Status	Domain	FSMO Role	Site
childdc1.second.rmad.local	GC	Bare Metal Active Directory Recovery	Completed s...	second.rmad.local		Default-First-Site-Name
dc1.rmad.local	GC	Bare Metal Active Directory Recovery	Completed s...	rmad.local		Default-First-Site-Name
DC2.rmad.local	GC	Install Active Directory From Media	Completed s...	rmad.local		Default-First-Site-Name

dc1.rmad.local

PREPARE TO START

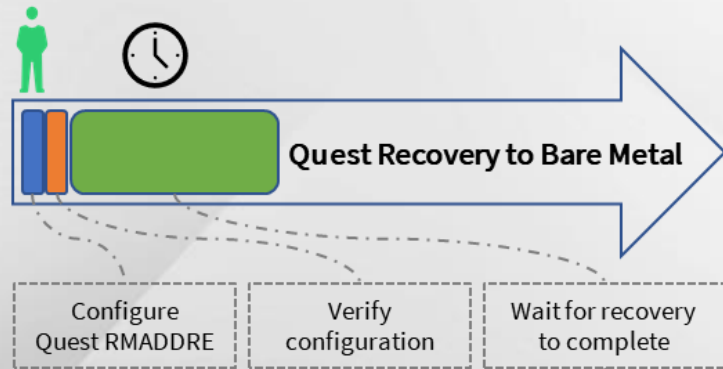
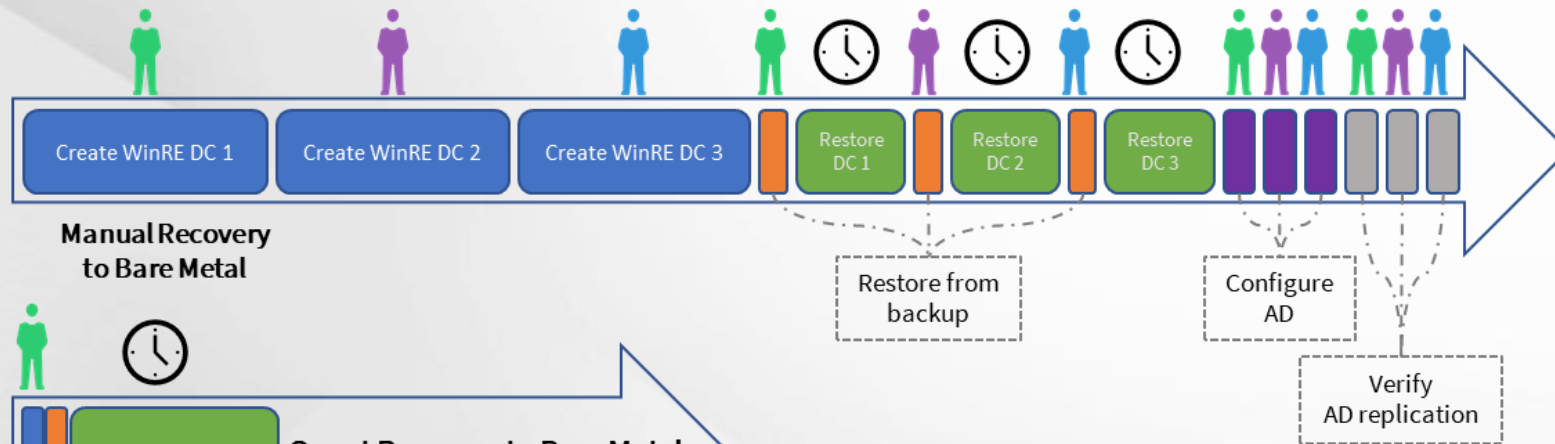
- ✓ Validate parameters 11/8/2018 3:39:03 PM
- ✓ Read computer network settings from backup 11/8/2018 3:39:04 PM
- ✓ Ensure that Quest Recovery Media is available 11/8/2018 3:39:04 PM
- ✓ Ensure that Forest Recovery Agent is installed and running 11/8/2018 3:39:10 PM
- ✓ Get information about computer 11/8/2018 3:39:12 PM



VERIFY RECOVERY PROJECT SETTINGS

- ✓ Run pre-recovery checks 11/8/2018 3:39:30 PM

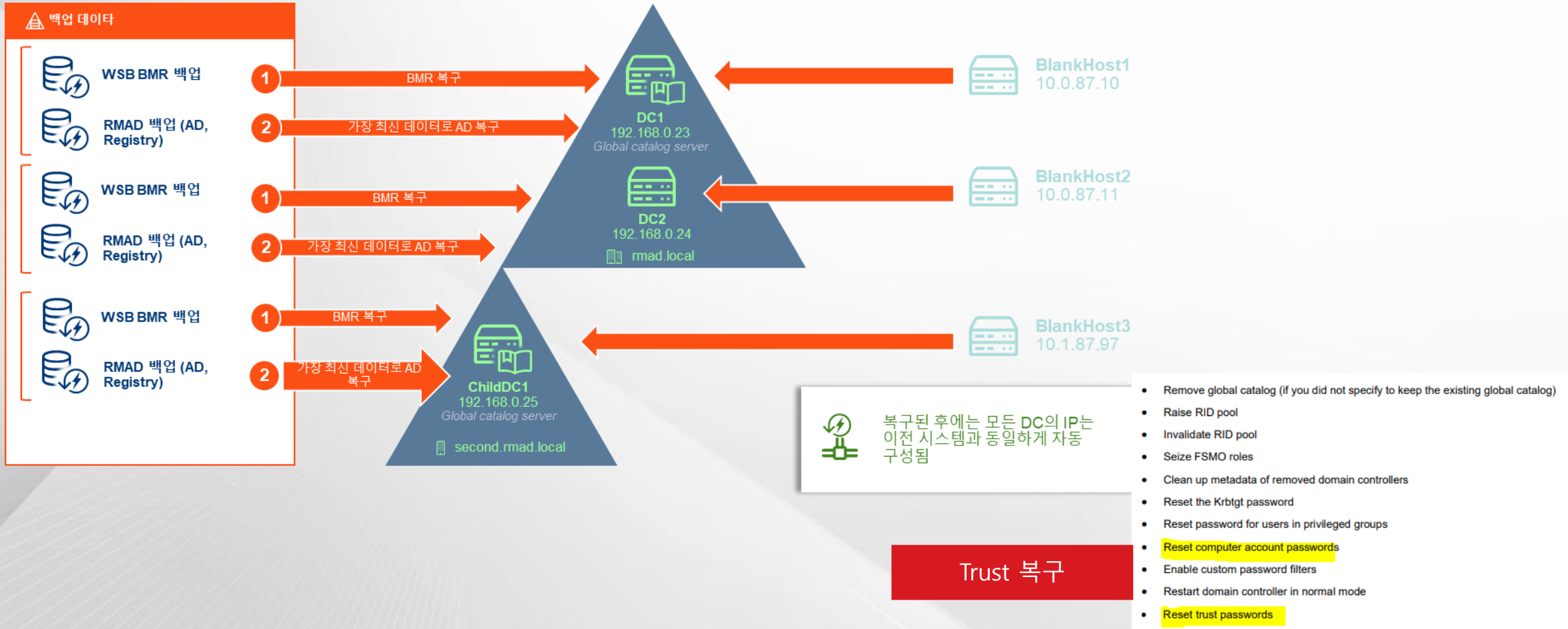
Forest에 대한 복구 Project 생성 및
주기적인 Validation 수행

2. 복구 시간



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

3. 데이터 Validation 및 Trust 복구



4. 다양한 복구 옵션 및 자동화된 복구 지원

다양한 복구 옵션 지원

- Restore Active Directory from backup method
- Install Active Directory method
- Reinstall Active Directory method
- Uninstall Active Directory method
- Restore SYSVOL
- Restore Active Directory on Clean OS method
- Bare Metal Active Directory Recovery method
- Do not recover method
- Do nothing method
- Adjust to Active Directory changes method

자동화된 복구 지원

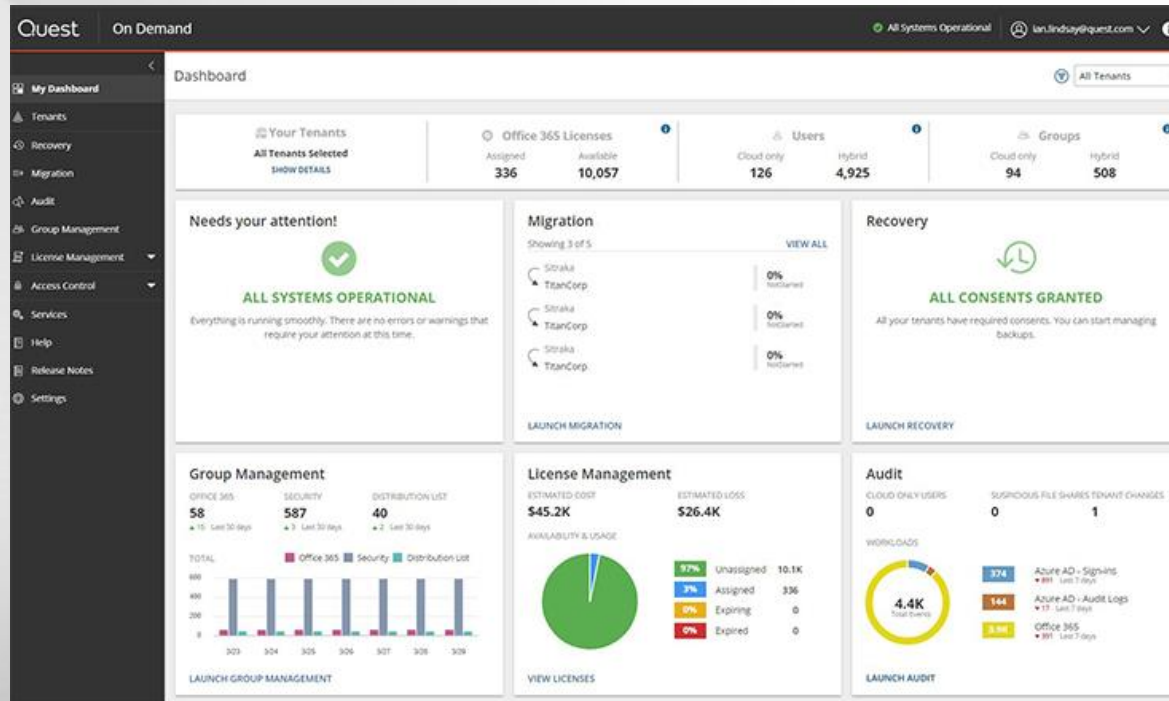
The screenshot displays the 'PREPARE TO START' and 'PERFORM RESTORE FROM BACKUP' sections of the Active Directory Recovery Wizard. The 'PREPARE TO START' section is completed, with three green checkmarks and timestamps: 'Get information about computer from backup' (3/5/2019 3:55:26 PM), 'Ensure that Quest Recovery Media is available' (3/5/2019 3:55:26 PM), and 'Wait for target machine booted from Quest Recovery Media' (3/5/2019 3:55:29 PM). The 'PERFORM RESTORE FROM BACKUP' section is currently active, showing a progress bar for 'Run pre-recovery checks'. Below this, a list of tasks is shown with radio buttons, including 'Restore disks from a Windows Server Backup', 'Configure Forest Recovery Agent on restored machine', 'Restart domain controller in DSRM mode', 'Disable Windows Update', 'Enable domain controller isolation', 'Bring all disks online', 'Copy the backup file to domain controller', 'Restore data from backup', 'Restart domain controller in normal mode', 'Disable custom filters for passwords', and 'Reset computer account passwords'. The 'CONFIGURE DOMAIN CONTROLLER' section is also visible, listing tasks such as 'Get information about computer', 'Select preferred DNS server', 'Remove global catalog if necessary', 'Raise RID pool', 'Invalidate RID pool', 'Seize FSMO roles', 'Clean up metadata of removed domain controllers', and 'Reset the Krbtgt password'.

AD복구는 단순히 파일 복구만으로는 안되고

- 18개의 핵심 설정이 적용 되어 함.
- 또한 40단계이상의 복구 프로세스로 구성됨

이러한 모든 과정을 자동화한 것이 RMAD

Hybrid 환경 지원



This table displays detailed information for each user, including their name, email, status, and any associated errors or warnings.

This table provides a detailed view of audit events, such as user logins, file share accesses, and system changes, with filters for date and severity.

- ✔ Office 365 licenses
- ✔ Mailbox
- ✔ Application role assignments
- ✔ Office 365 groups & Teams membership
- ✔ Multi-factor authentication & password reset configuration
- ✔ Azure AD Roles membership
- ✔ Conditional Access Policies rules
- ✔ Custom properties for cloud applications
- ✔ SharePoint permissions

“완벽한 데이터 복구 지원”



감사합니다.