

Securing Identities and Recovering Faster

in the Age of Ransomware

ADRIA Forum 2026

Quest Software

BURCU MERIC

Enterprise Sales Manager /South East Europe & Turkey

Protect identity. Detect compromise. Recover trust. Restore the business.

What do you recover first?

Imagine it's Monday morning.

Your users can't log in.

Administrators can't authenticate.

Servers are going offline.

Your security team discovers that
privileged credentials have been compromised .

And your Active Directory environment can no longer be trusted.



Question: What do you recover first?

Servers?? Storages?? Files?? VMs?? Databases?? Applications?? etc

What do you recover first?

Answer: None of them.

YOU MUST RECOVER IDENTITY FIRST.

You can recover a server.

You can recover a database.

You can recover a VM.



**But if you cannot establish who is trusted, who can authenticate,
and who is authorized — you cannot securely bring the environment back online.**

Ransomware has changed the recovery question

- The attacker's objective is not only to encrypt data — it is to control the environment.
- Compromised credentials and privileged identities can become the route to critical systems.
- If identity services are compromised, restoring servers alone may not restore business operations.
- The real question: **Can we recover a trusted identity foundation quickly?**



IDENTITY

DATA

APPS

Identity is a high-value target

- Active Directory and Entra ID often sit at the center of authentication, authorization and administration.
- Attackers can abuse legitimate credentials and trusted paths to move through the environment.
- Tier 0 assets — domain controllers, privileged groups and identity infrastructure — can determine the blast radius.
- Identity security therefore has to cover **prevention, detection, response and recovery**.



Protect the keys to the kingdom — and know how to rebuild them.

A cyber-resilience lifecycle for identity



**The goal is not simply to survive an attack.
It is to reduce the time between compromise and trusted business operations.**

What does “identity recovery” actually mean?

- **Identify** a last known trusted state.
- **Protect** recovery data from the same attack.
- **Validate** backups and recovery plans.
- **Rebuild** the forest/domain in a controlled sequence.
- **Verify** authentication, replication, trusts and critical services.

Trusted backup

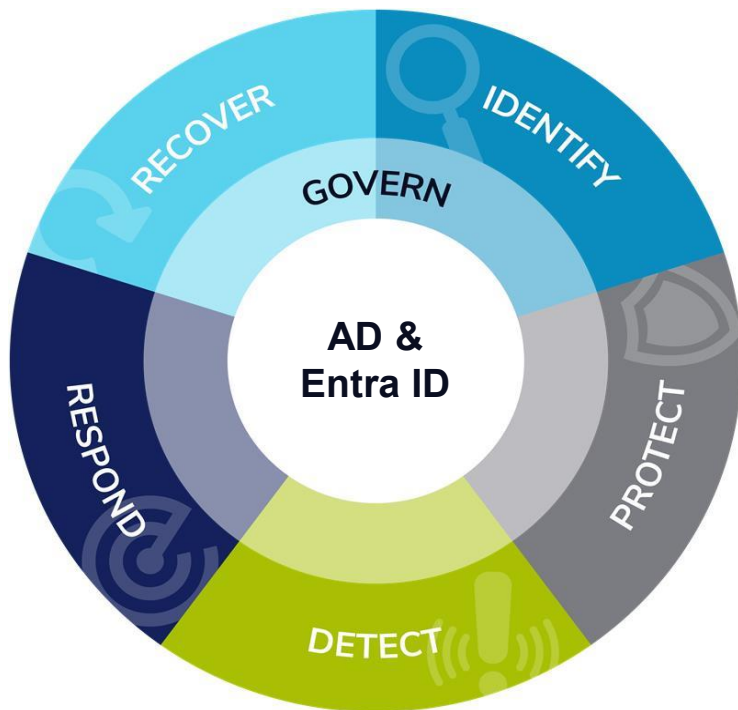
Clean recovery

Forest health

Business restored

Where Quest Supports Customers: Quest Security and Resilience

Unmatched defense in depth | Mapped to NIST & Gartner ITDR



Identify

Assess risk and limit attack surface. Describes visibility of your environment. What are the Tier zero objects, do you have visibility of who has access to what



Protect

Prevent changes to critical identity assets
Lock your environment and prevent //internal ,external attackers



Detect

Monitor and audit threats in real time.
What is changed, is the change critical



Respond

Contain security events quickly & investigate root cause
Being able to drive investigation // single pane or multiple tools?



Recover

Restore hybrid identity quickly to reduce downtime
How easily you can recover?
Once AD gone, can you be able to report what users have Done?

Quest Security Management Platform

Quest Identity
Defense

Quest Identity
Recovery

Quest Change Auditor: know what changed

- Real-time auditing across Active Directory and hybrid Microsoft environments.
- Track critical user, group, GPO and configuration changes.
- Detect indicators of compromise and suspicious activity.
- Correlate events to accelerate investigation and forensics.
- Protect critical objects and roll back unauthorized changes.



Easy to read, normalized 5W events

Change Auditor [connected to MGMT2.demosure.com - DEFAULT] as user [Administrator (DEMOSURE)]

File Edit Action View Help

Start Overview Searches Administration Tasks

Overviews Event Details Print

My Favorite Search: Change Auditor Real-Time

Run on: 10/11/2023 10:31 AM Run Time: 00:00:00
Next Refresh: 10/11/2023 10:36 AM Records: 2219 Refresh

Drag a column header here to group by that column.

Severity	Time Detected	Subsystem	User	Event	Computer	Action	Domain	Result
Click here to filter data...								
Medium	10/11/2023 10:25...	SQL	sa	Missing Column Statistics	SQL1	Other	DEMOSURE	None
Medium	10/11/2023 10:25...	SQL	sa	Missing Column Statistics	SQL1	Other	DEMOSURE	None
Medium	10/11/2023 10:24...	SQL	NT SERVICE\...	Audit Logout	SQL1	Other	DEMOSURE	None
Medium	10/11/2023 10:24...	SQL	NT SERVICE\...	Audit Login	SQL1	Other	DEMOSURE	None
Medium	10/11/2023 10:24...	SQL	NT SERVICE\...	Audit Login	SQL1	Other	DEMOSURE	None
Medium	10/11/2023 10:24...	SQL	NT SERVICE\...	Audit Logout	SQL1	Other	DEMOSURE	None
Medium	10/11/2023 10:24...	Active Direc...	DEMOSURE\Ad...	User member-of added	DC1	Add Attribute	DEMOSURE	Success
Medium	10/11/2023 10:24...	Active Direc...	DEMOSURE\Ad...	Member added to group	DC1	Add Attribute	DEMOSURE	Success
Medium	10/11/2023 10:24...	Active Direc...	DEMOSURE\Ad...	Member added to group	DC1	Add Attribute	DEMOSURE	Success
Medium	10/11/2023 10:24...	Active Direc...	DEMOSURE\Ad...	User member-of added	DC1	Add Attribute	DEMOSURE	Success
High	10/11/2023 10:24...	Active Direc...	DEMOSURE\Ad...	Nested member added to critical enterprise group	DC1	Add Attribute	DEMOSURE	Success
High	10/11/2023 10:24...	Active Direc...	DEMOSURE\Ad...	Member added to critical enterprise group	DC1	Add Attribute	DEMOSURE	Success
Medium	10/11/2023 10:24...	Active Direc...	DEMOSURE\Ad...	Nested member added to group	DC1	Add Attribute	DEMOSURE	Success
Medium	10/11/2023 10:24...	Active Direc...	DEMOSURE\Ad...	Nested member added to group	DC1	Add Attribute	DEMOSURE	Success
Low	10/11/2023 10:23...	AD Query	DEMOSURE\Ad...	AD Query Performed	DC1	Other	DEMOSURE	Success
Medium	10/11/2023 10:23...	Active Direc...	DEMOSURE\Ad...	Office changed on user object	DC1	Modify Attribute	DEMOSURE	Success
Medium	10/11/2023 10:23...	Active Direc...	DEMOSURE\Ad...	Office changed on user object	DC1	Add Attribute	DEMOSURE	Success
High	10/11/2023 10:22...	SQL	DEMOSURE\Ad...	Table Removed	SQL1	Delete Object	DEMOSURE	None
Medium	10/11/2023 10:22...	SQL	DEMOSURE\Ad...	Primary Key Removed from a Table	SQL1	Delete Object	DEMOSURE	None
Medium	10/11/2023 10:22...	SQL	DEMOSURE\Ad...	Object Renamed	SQL1	Rename Object	DEMOSURE	None

Copy Email... Print Knowledge Base... Comments... Disable Related Search Protect

Medium Severity

Who: DEMOSURE\Administrator (Administrator) ← Who

Where: DC1 ← Where

What: The office was changed from Chicago to New York for user CN=John Doe,OU=Synced Users,DC=demosure,DC=com.

Active Directory

Class: user

Object: demosure.com/Synced Users/John Doe

From: Chicago ← Before and after values

To: New York ← Before and after values

What: ← What

When Workstation → When: 10/11/2023 10:23:35 AM

Origin: DC1.demosure.com (10.0.0.1)

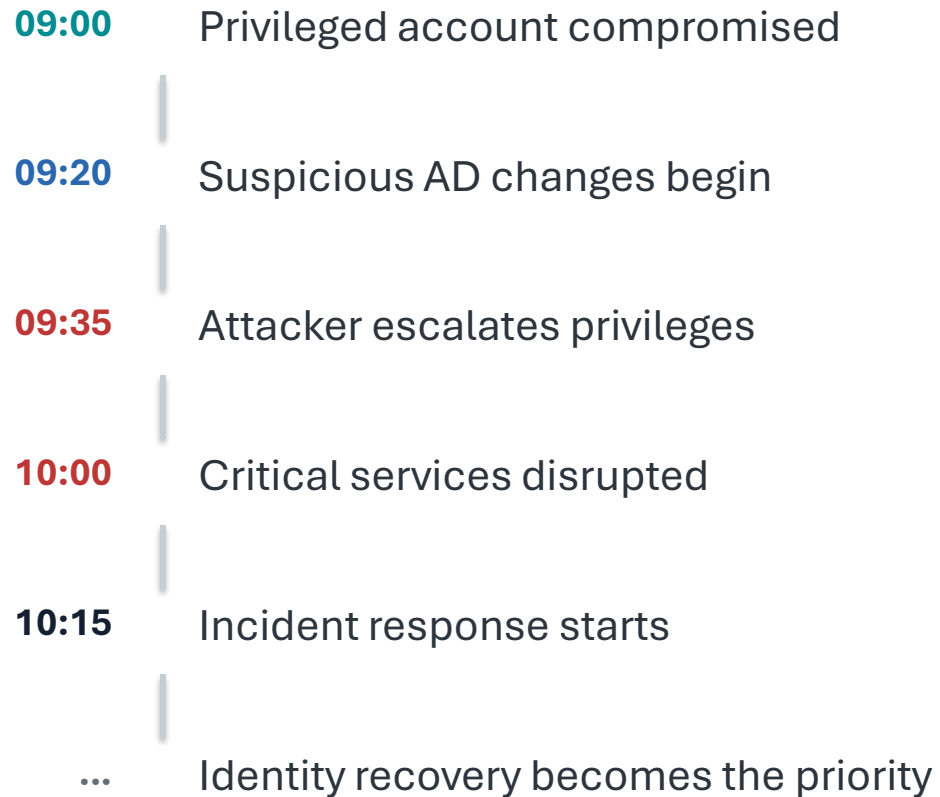
Result: Success

Facility: Custom User Monitoring

Authentication: Kerberos

Port: 389

A ransomware scenario: from compromise to recovery



Question: How long to trusted operations?

Quest Recovery Manager for Active Directory:

Recover the identity foundation

- Back up the Active Directory data needed for recovery.
- Support granular restores as well as domain and forest recovery.
- Use integrity checks and malware scanning to help validate recovery data.
- Automate the complex sequence of forest recovery operations.
- Support phased recovery and multiple recovery approaches.

RECOVERY MANAGER

- ✓ Trusted backup
- ✓ Automated recovery
- ✓ Forest health checks

Recovery is a process — not a backup file.

Recovery must be trustworthy — not just fast

TRUST

Use known-good recovery points
and verify recovery data

ISOLATE

Keep recovery resources
protected from the production attack

AUTOMATE

Reduce manual steps,
errors and recovery time

VALIDATE

Check forest health,
replication and authentication

Fast recovery *without trusted identity is not recovery.*

The takeaway

**Ransomware resilience is
identity resilience.**

Protect the identity.

Detect the compromise.

Recover trust — and restore the business.

Quest helps customers secure, monitor, respond to and recover their Microsoft identity environments.

THANK YOU

BURCU MERIC

**Quest Software-Enterprise Sales Manager
South East Europe & Turkey**

Email: Burcu.meric@quest.com

Mobile: +90 533 144 97 93