# Can your ITDR do more than detect?

Unify identity defense, recovery, and modernization — so security doesn't stop during change.

**80%**

80%+ of attacks are malware-free credential abuse

Privilege escalation happens in minutes after identity compromise

**75%**

75%+ don't test identity disaster recovery often enough

## 1

THE SECURITY REALITY

## Identity attacks bypass traditional detection models

- Identity is the primary attack surface
- Detection-only controls can't stop identity-based compromise
- AI accelerates attacks and multiplies non-human identities
- Untested recovery assumptions create board-level and regulatory risk

## 2

THE DETECTION-ONLY GAP

## Seeing identity threats is not the same as stopping them

- Alerts without containment or coordinated response
- Increased outage risk with manual or untested recovery
- Security controls weakened during migration
- No measurable resilience

## 3

WHY THE GAP IS GROWING

## ITDR is expanding — and identity risk spikes during change

ITDR is evolving beyond detection to full lifecycle security

Cloud, AI, Zero Trust, and M&A accelerate identity modernization

## Security cannot pause during migration, modernization, or M&A

## 4

THE QUEST ANSWER

## A unified platform for full-lifecycle ITDR

### What you need

Security leaders need a single platform that reduces identity risk, contains attacks, and enables fast recovery using consistent controls across everyday operations and periods of change.

### What Quest delivers

Quest Security Management Platform unifies identity defense, recovery, and modernization across hybrid Active Directory and Entra ID environments

## 5

HOW IT WORKS

## Continuous identity protection before, during, and after compromise

**Before compromise:**

- Reduce identity exposure
- Protect Tier 0 assets and privileged paths

**During an incident:**

- Deploy Shields Up containment to limit blast radius
- Protect crown-jewel identity assets

**After compromise:**

- Restore trust with automated, tested recovery

**During modernization:**

- Drive secure migrations and identity modernization by design

## 6

Platform Pillars

## Five pillars of unified identity security and ITDR

1. **Proactive Identity Defense** — Actively block identity-based attacks
2. **Deep AD/Entra ID visibility** — Monitor human and non-human identities
3. **Attack-Tested Identity Recovery** — Automate recovery at enterprise scale
4. **Security-First Modernization** — Secure migrations, without weakening posture
5. **Unified ITDR Platform** — Manage one control plane aligned to NIST CSF 2.0

## 7

MEASURABLE OUTCOMES

## Proven identity resilience outcomes

**44%**

44% improvement in identity MTTR

**90%**

Up to 90% faster identity recovery

**$19.7M**

Reduced ransomware blast radius and $19.7M in potential savings

## 8

## Move beyond detection-only ITDR

Unify identity defense, containment, recovery, and secure modernization on one platform — so identity security and resilience remains continuous, even during moments of greatest change and risk.

Learn more about the
**Quest Security Management Platform**

Learn more →

Quest and the Quest logo are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit www.quest.com/legal/trademark-information.aspx. All other trademarks are property of their respective owners © 2026 Quest Software Inc. ALL RIGHTS RESERVED.

quest.com