Qualys ETM Identity

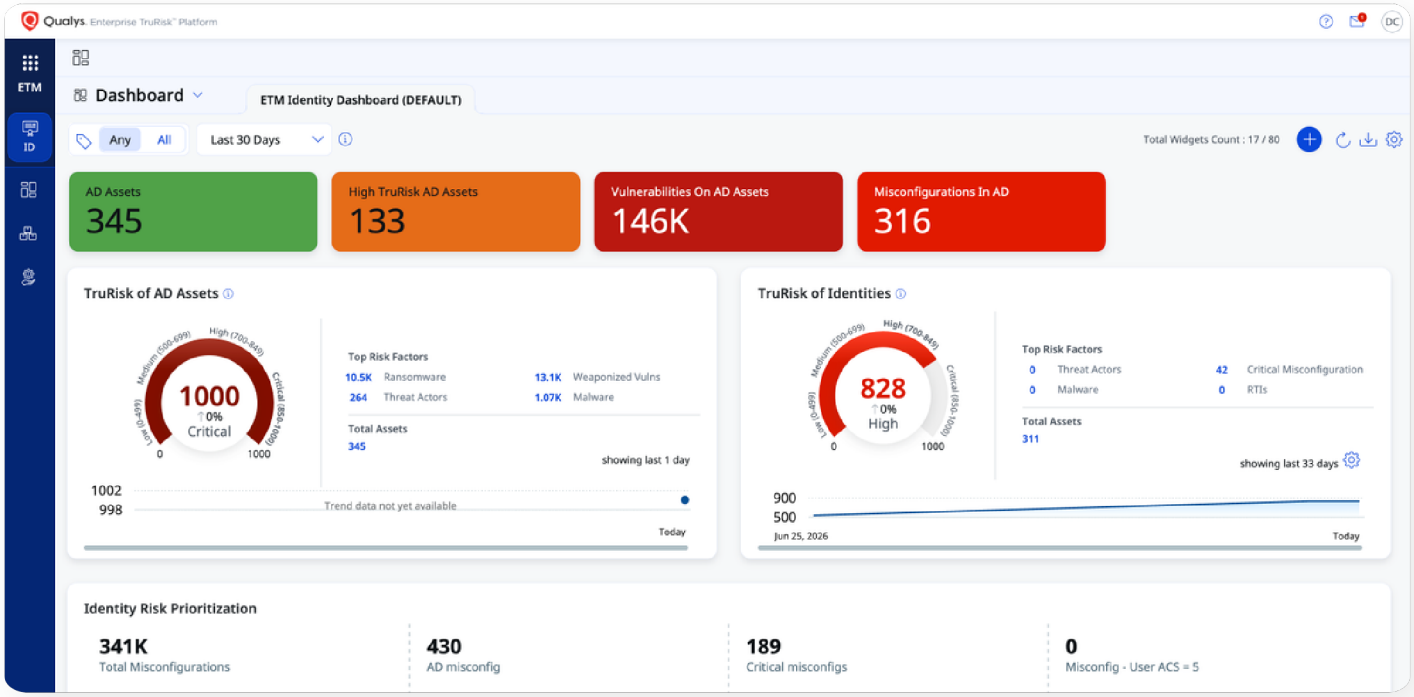
Transform identity intelligence into prioritized action with complete attack path visibility and contextual risk.

Where Traditional Identity Security Falls Short

Typically enterprise identity program is built on three layers: Identity and Access Management (IAM) to control who can sign in, Identity Governance and Administration (IGA) to govern and certify that access over time, and Privileged Access Management (PAM) to lock down the most privileged accounts. None of them, on its own or together, continuously ask whether access already granted is still safe. An IGA certification from six months ago doesn't account for an attack path that opened last week; a PAM vault protects the privileged accounts already known about, not the shadow admin nobody classified as privileged in the first place.

Meanwhile, identities span on-premises Active Directory (AD), Entra ID, and Okta, each governed by its own tools and reviewed on its own audit cycle, weeks behind the attacker. This is the gap Identity Security Posture Management (ISPM) exists to close — by continuously detecting identity misconfigurations and related security risks. Qualys ETM Identity delivers these capabilities by correlating identity posture with asset risk and orchestrating remediation.

How Qualys ETM Identity Enables Continuous Posture Management



Built into the Qualys Enterprise TruRisk™ Management (ETM) platform, Qualys ETM Identity provides the continuous identity security layer that complements existing IAM, IGA, and PAM investments. Rather than replacing your identity stack, it brings identity risk into the same board-ready TruRisk™ reporting already trusted for vulnerabilities and misconfigurations. Qualys ETM Identity delivers continuous identity posture management through three core capabilities:

Measure

Continuously discover and assess every identity across AD, Entra ID, and Okta, exposing posture, attack paths, and misconfigurations that periodic reviews miss.

Communicate

Correlate identity findings with asset context to quantify business risk through Identity TruRisk™, so teams and executives prioritize using a common risk language.

Eliminate

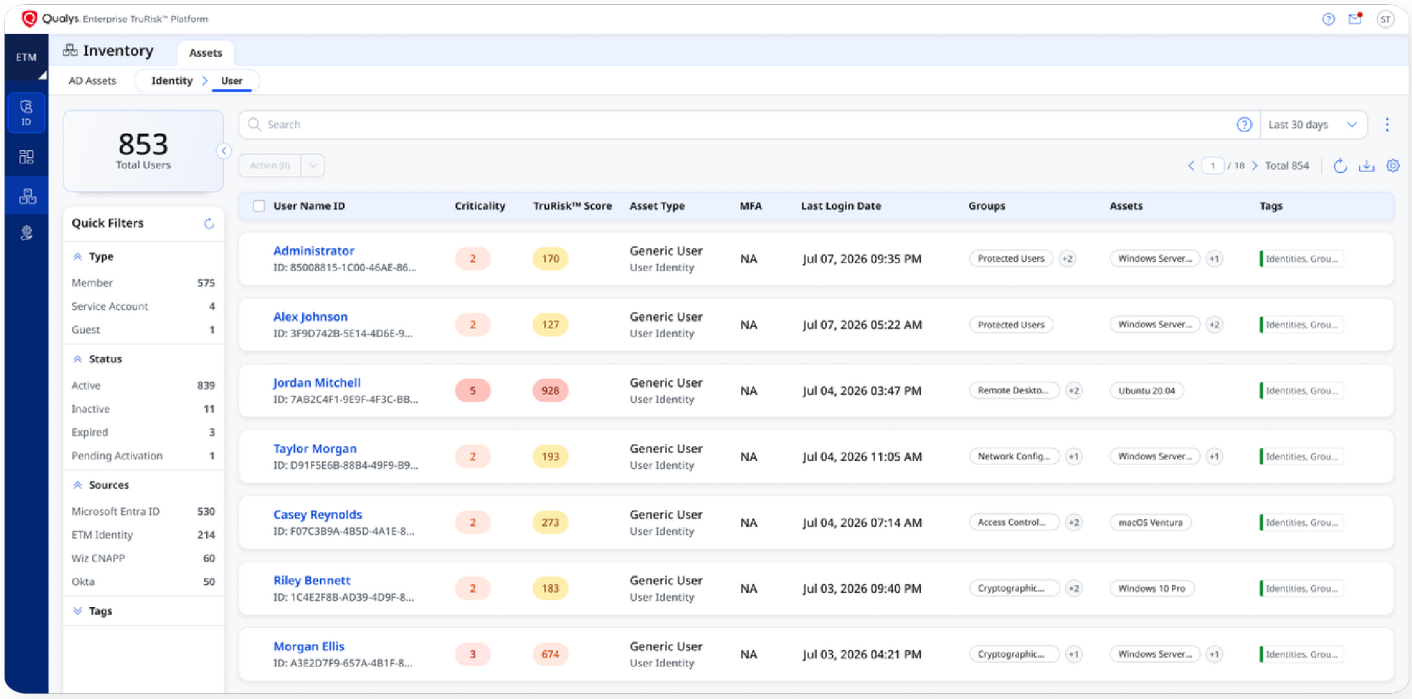
Guide teams with contextual remediation recommendations, validated risk reduction, and continuous compliance mapping, while preserving existing IAM, IGA, and PAM workflows.

Key Use Cases for Qualys ETM Identity

01 Unified Identity Inventory

Users, groups, and service accounts are scattered across on-premises AD, Entra ID, and Okta, with local Windows and service accounts often going completely unaccounted for. **Identity Inventory** and **Unified Asset Inventory (UAI)** unify every identity into one view — including roles and misconfiguration findings from AD, Entra ID, and Okta — enriched with TruRisk™, criticality, and access context, the moment a directory or identity provider connects. **Qualys Cloud Agent** provides the deepest Active Directory risk coverage by leveraging PowerShell-based collection, while the **Agentless AD Connector** uses LDAP interfaces to provide foundational identity visibility for domain controllers where agents cannot be deployed. **Local Identities Support** discovers the Windows and service accounts that no cloud identity provider ever reaches.

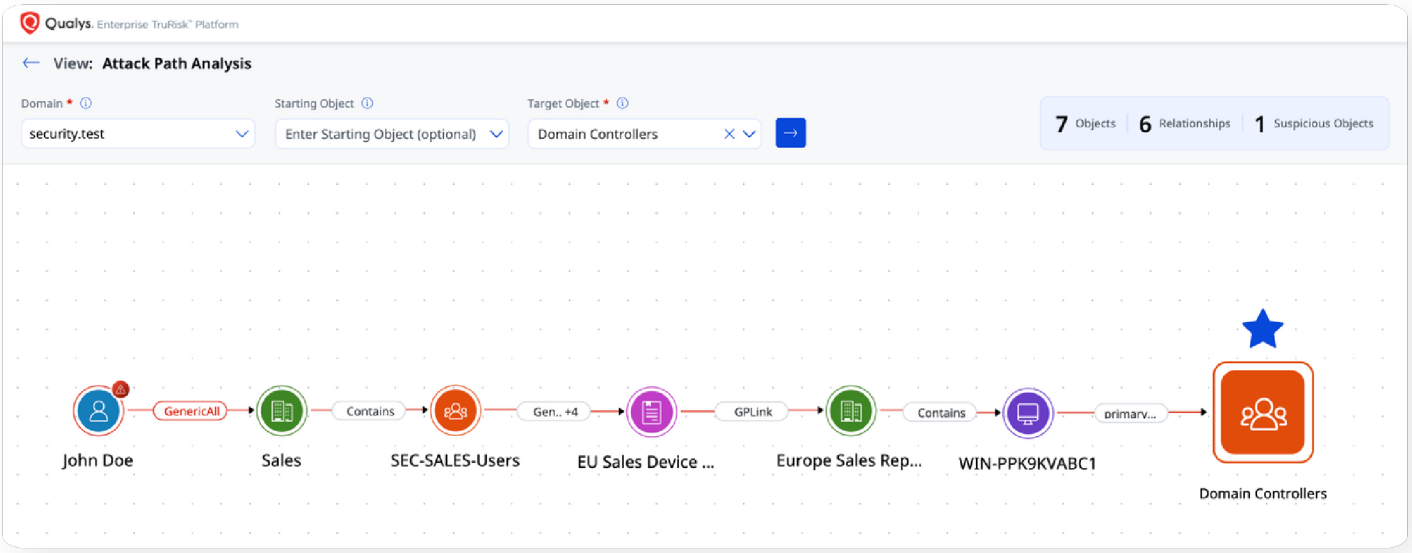
Outcome: Teams get one authoritative inventory of every identity — human, machine, shadow, cloud, and on-premises — in place of the spreadsheets most still rely on.



02 Attack Path Detection and Analysis

Individual permissions rarely look dangerous alone. Chained together across group memberships, Group Policy Object (GPO) rights, and delegated access, they can hand an attacker a direct route to Domain Admin — and most organizations can't see that chain until it's exploited. **AD Attack Path Analysis** maps how permissions chain together, the same way an attacker would trace them. **AI Attack Path Summarization** explains the chain in plain language with severity ratings on each relationship, **AD Attack Path Findings** maps it to the exact accounts responsible and ranks it by asset criticality and technical debt, and **AD Blast Radius Analysis** shows the blast radius of compromised identities before attackers reach Tier-0 assets and Domain Controllers.

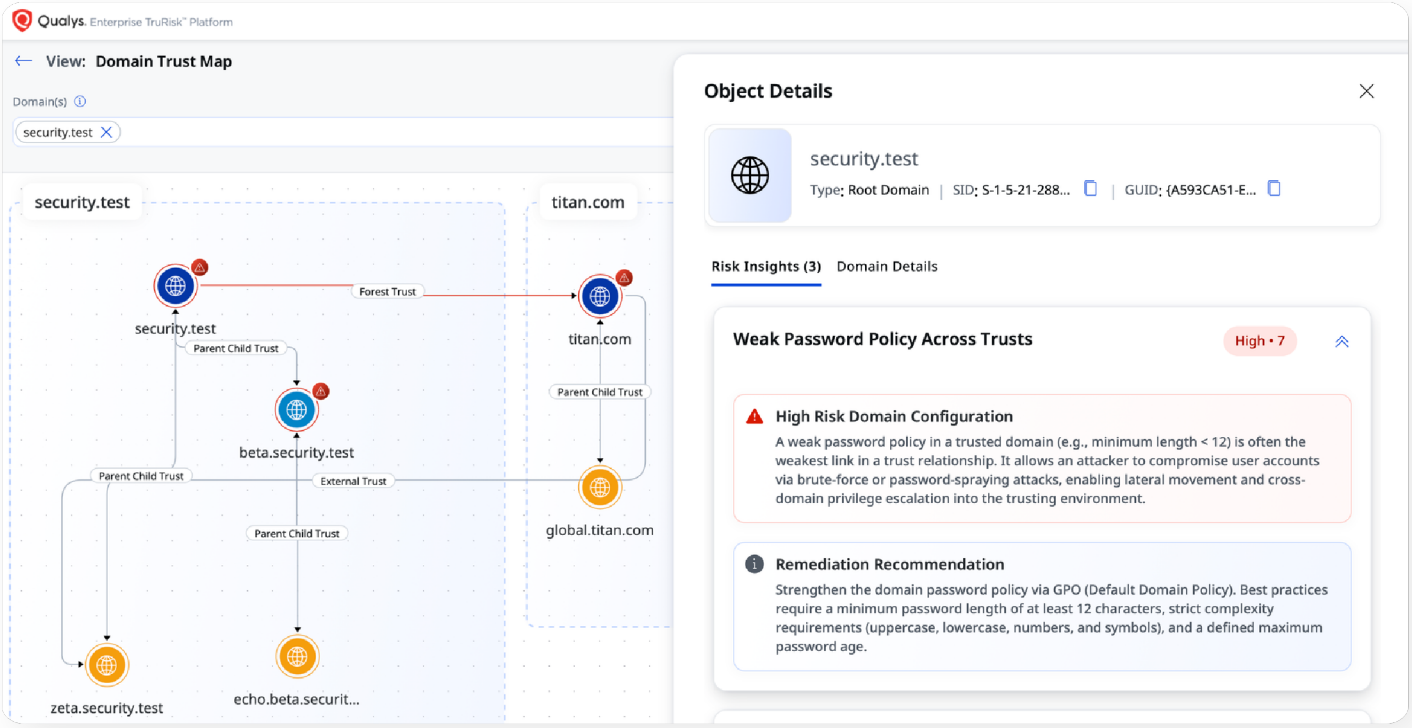
Outcome: Attack paths and lateral movement routes identified and prioritized before they're used, not discovered afterward during incident response.



03 Domain Trust Visibility and Hardening

Trust relationships between domains and forests are exactly the infrastructure attackers use to move laterally, but they're typically configured once and never reviewed again, letting external or orphaned trusts persist for years unnoticed. **Domain Trust Map** visualizes every parent-child, forest, external, and shortcut trust across your AD forest, with an environment-wide summary of how many forests, domains, and trust relationships exist. **Domain Trust Findings** converts the risky ones into remediation-ready items, and **Foreign Security Principal Support** identifies external users and groups with granted access and surfaces orphaned trusts left behind by broken relationships.

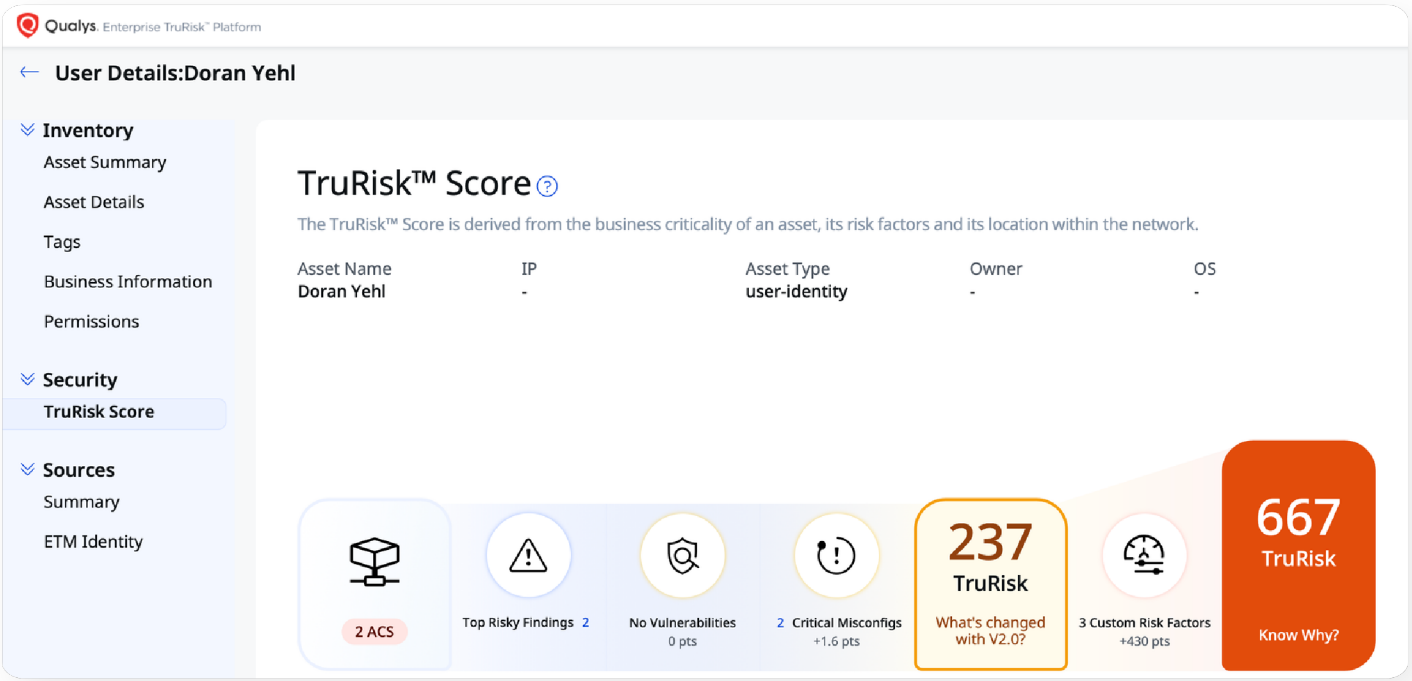
Outcome: Every risky trust relationship ranked for hardening or cleanup, with blast radius assessed across every trusted domain — collapsing an attack surface usually found mid-incident.



04 Identity Risk Quantification and Prioritization

Identity misconfigurations, excessive privileges, and toxic permission combinations generate more findings than any team can triage manually — and without a shared risk language, identity issues compete for attention against vulnerabilities tracked elsewhere. **Identity TruRisk™** scores every identity by business context and asset criticality, not just a count of findings, with AD, Okta, and Entra ID each surfacing their own top risk factors. **Identity Criticality Scoring** lets administrators assign business importance at scale; **Identity Insights** correlates privileged users, MFA gaps, stale accounts, and toxic permission combinations into that same score, and **Identity Misconfigurations** maps every finding to MITRE ATT&CK, enriched with 25+ threat-intelligence and directory sources. **AD Real-Time Monitoring** flags suspicious logons, privilege escalation, MFA disablement, and policy tampering the moment they happen.

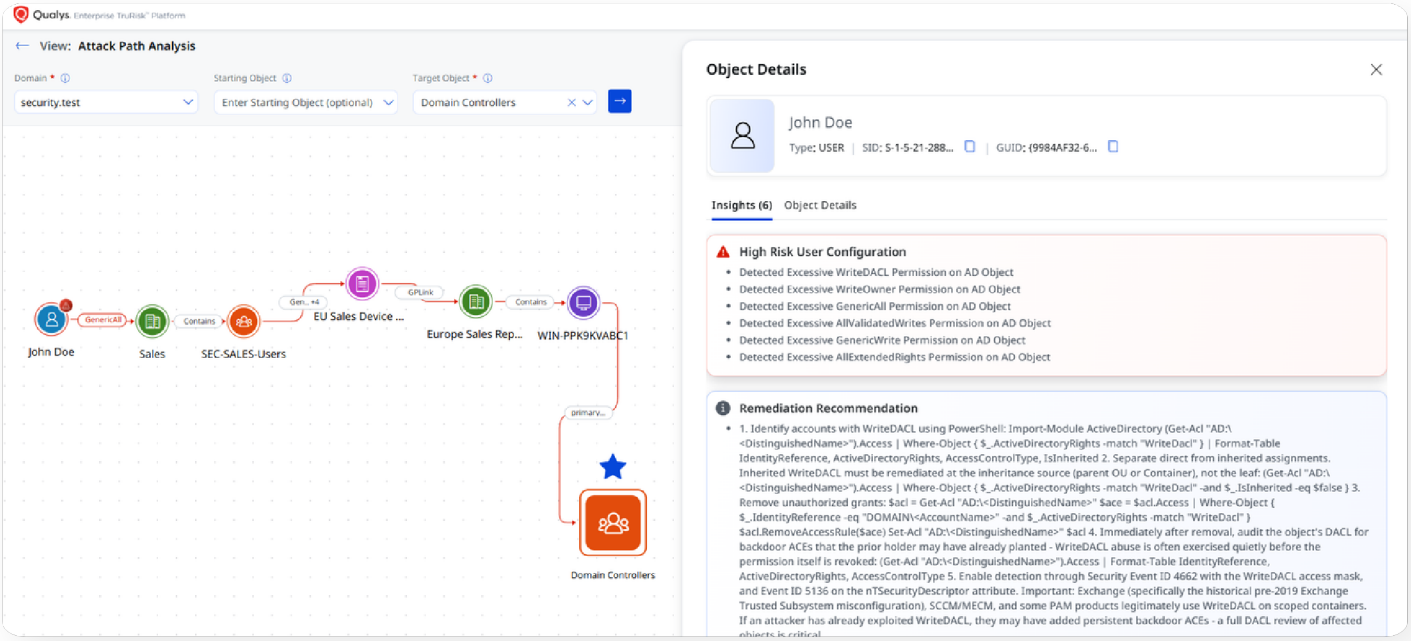
Outcome: Identity risk prioritized by what it's actually attached to, with full who-changed-what-and-when attribution the moment something happens.



05 Continuous Identity Audit Readiness

Fixing identity risk and proving it was fixed are usually two separate, manual efforts — and mapping identity findings to compliance frameworks is typically repeated from scratch for every audit cycle. **Remediation Guidelines** recommend the fix, drawing on 200+ built-in AD policy controls and one-click actions — enforcing MFA, de-privileging, disabling, or removing a toxic permission — with fixes confirmed and reflected in an updated Identity TruRisk™ score. **Risk Acceptance Workflow** preserves audit visibility on any accepted exception, and **Qualys** continuously assesses identity risks against security benchmarks including DISA STIG, CIS, HIPAA, PCI-DSS, and GDPR, helping organizations maintain compliance readiness with audit trails and dashboards.

Outcome: Confirmed risk reduction and non-repudiable audit evidence that already exists when the audit starts, supporting Zero Trust initiatives.



Secure Your Identity Attack Surface for the Frontier AI Era

Continuously discover, prioritize, and remediate identity attack paths — with contextual insights and a unified view across your hybrid environment.

Start Free Trial

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of disruptive cloud-based Security, Compliance and IT solutions with more than 10,000 subscription customers worldwide, including a majority of the Forbes Global 100 and Fortune 100. Qualys helps organizations streamline and automate their security and compliance solutions onto a single platform for greater agility, better business outcomes, and substantial cost savings. Qualys, Qualys VMDR® and the Qualys logo are proprietary trademarks of Qualys, Inc. All other products or names may be trademarks of their respective companies.

For more information, please visit **qualys.com**

©2026 Qualys, Inc. All Rights Reserved.