Identity Threat Detection and Response (ITDR)

Stay ahead of identity-based threats by proactively remediating risks, blocking attacks, detecting and responding in real-time, and ensuring rapid recovery of your vital identity system.

Netwrix Identity Threat Detection and Response (ITDR) empowers enterprises to stay ahead of identity-based threats by eliminating risks before they can be exploited. It blocks risky changes, enforces strong security controls, and detects even sophisticated identity attacks in real-time. With automated response and rapid AD forest recovery, threats are contained before they escalate, minimizing disruption and ensuring resilience against identity-driven attacks.

REDUCED SECURITY RISK

Prevent breaches by proactively uncovering and remediating risks and misconfigurations. Block risky changes and privilege escalation—stopping attackers in their tracks.

ACCELERATED THREAT DETECTION AND RESPONSE

Detect in real-time even the stealthiest threats lurking in AD and Entra ID. Instantly neutralize threats with automated response actions before they escalate.

MINIMIZED DOWNTIME AND BUSINESS DISRUPTION

Ensure business continuity by quickly reversing unwanted changes and recovering deleted objects. Strengthen AD resilience with automated forest recovery, restoring operations fast.

> **Excellent product and provides protections that other companies cannot. Monitoring solutions is not enough these days, you need to have the ability to stop threats in their tracks. None of the other vendors do more than just monitor and alert.**
>
> IT Security and Risk Management, Banking

Netwrix PingCastle Enterprise

Netwrix Threat Manager

- Active Directory & Entra ID

Netwrix Threat Prevention

- Active Directory
- Enterprise Password Enforcer
- LDAP

Netwrix Access Analyzer

- Active Directory & Entra ID
- AD Permissions Analyzer
- Active Directory Actions

Netwrix Recovery for AD

- Object & Attribute Level
- Forest Level

Safeguard your Identity Infrastructure

IDENTIFY WEAKNESSES IN YOUR ACTIVE DIRECTORY

Reduce exposure to identity-based attacks by identifying critical security gaps across your AD and Entra ID infrastructure before attackers do. Strengthen your security posture by uncovering shadow attack paths and privilege weaknesses that create hidden entry points for adversaries.

PREVENT THREATS

Prevent identity compromise by creating a security perimeter around critical directory assets, blocking unauthorized modifications to Tier 0 assets. Reduce the risk of lateral movement by stopping privilege escalation attempts at the source, keeping attackers from compromising your environment.

AUTOMATE THREAT RESPONSE

Respond to threats instantly with automated response actions that stop attackers in their tracks, such as killing suspicious sessions or disabling compromised accounts. Streamline operations through integrations with leading SIEM solutions, ServiceNow, Slack, and Microsoft Teams, putting critical threat intelligence exactly where your security teams already work.

REMEDIATE UNWANTED AD CHANGES

Minimize downtime and security risks by instantly rolling back accidental or malicious changes and recovering deleted AD objects with precision. Effortlessly restore users, computers, GPOs, DNS entries, and more. Real-time change intelligence enables swift, informed decision-making, empowering IT teams to respond to incidents confidently and maintain operational continuity.

REMEDIATE RISKS

Reduce your identity attack surface by eliminating dangerous misconfigurations, stale objects, and toxic permission conditions in bulk and at scale. Enhance security by enforcing least privilege principles and strong password policies across your enterprise identity ecosystem without burdening your team.

DETECT THREATS IN REAL-TIME

Detect AD and Entra ID attacks in real time and prevent headline-making breaches. Deploy deceptive honeytokens to expose attackers early in their kill chain or leverage machine learning powered User Behavior Analytics (UBA) to pinpoint truly malicious activity that traditional tools miss.

INVESTIGATE IDENTITY-BASED ATTACKS

Simplify complex investigations with complete attack timelines that connect all related events. Rapidly analyze the scope and impact of identity-based threats with contextual visibility into attacker techniques, compromised assets, and affected resources to accelerate remediation efforts.

AUTOMATE AD FOREST RECOVERY

Ransomware and system failures can bring your business to a halt. Avoid weeks of downtime with fully automated AD forest recovery in minutes or hours. Netwrix Recovery for AD restores your identity infrastructure fast, eliminating complex manual steps for a smooth, reliable recovery.

WHY NETWRIX?

PATENTED INNOVATION

Leverage industry-leading, patented technologies for advanced threat detection and attack blocking, delivering unmatched identity security for your Active Directory and Entra ID environments.

COMPLETE PROTECTION

The most comprehensive ITDR solution — securing AD and Entra ID through risk assessment and remediation, threat prevention, real-time detection, automated response, and recovery, minimizing disruption and maintaining business continuity across hybrid environments.

FLEXIBLE AND SCALABLE

Delivers seamless identity threat protection for large, complex IT environments while scaling effortlessly to support mid-sized organizations without added complexity.

Next Steps

REQUEST ONE-TO-ONE DEMO | REQUEST A QUOTE

Corporate Headquarters: 6160 Warren Parkway Suite 100, Frisco, TX, US 75034

Phone: 1-949-407-5125 **Int'l:** 1-949-407-5125 **Toll-free:** 888-638-9749 **EMEA:** +44 (0) 203-588-3023

netwrix.com/social