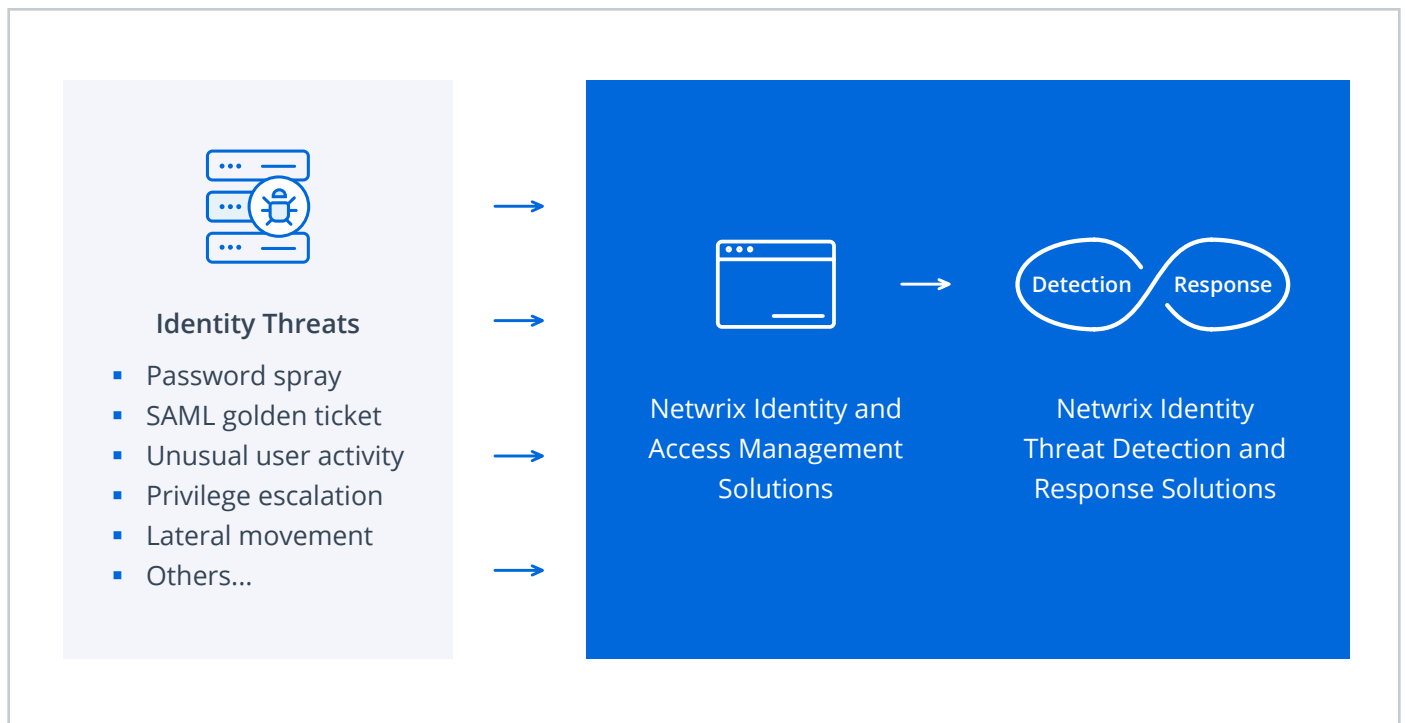


Identity Threat Detection and Response: Why Netwrix

An abstract graphic with a dark blue background. It features a network of glowing blue and purple nodes connected by thin lines, creating a complex web-like structure. The nodes are scattered across the lower half of the image, with some lines extending upwards towards the text.

Introduction

Your user accounts are a prime target for adversaries because compromising a single identity gives them a foothold in your IT ecosystem that they can use to steal sensitive data and damage vital systems. To defend against these attacks, organizations need a comprehensive approach to identity threat detection and response (ITDR). Indeed, Gartner includes ITDR as one of its [“7 Top Trends in Cybersecurity for 2022.”](#)



The Netwrix Approach to Identity Threat Detection and Response

Netwrix offers a comprehensive ITDR strategy to protect your identities and identity infrastructure. Netwrix solutions empower you to:

- **Detect** identity threats in their early stages by continuously monitoring for suspicious activity, such as indicators of [DCShadow](#) or [password spraying](#) attacks.
- **Respond** instantly to attacks by automatically executing a predefined playbook that could, for example, disable the suspicious account, reset its password and alert the security team.
- **Recover** fast to minimize costly downtime.

Let's dive deeper into these capabilities.

Detect

Get alerted to identity threats. Know right away about activity that might put your organization's security at risk by setting up real-time alerts on the events you consider critical. You can even proactively block risky changes and known attack techniques like [enumerating AD users](#).

Uncover malicious actors. Pinpoint truly suspicious activity using advanced machine learning, and lure attackers into revealing themselves with honey tokens that look like legitimate credentials.

Detect even advanced identity attacks. Threat actors leverage increasingly sophisticated techniques to stay under the radar, but Netwrix solutions bring them into the light with real-time detection of [Golden Ticket](#), [Kerberoasting](#) and many other attacks.

Respond

Contain threats automatically. Respond instantly to expected identity threats by setting up playbooks that take actions such as automatically locking the offending account and forwarding the details to your SIEM, ITSM or other security platform.

Accelerate investigations and harden security. Analyze detailed event information in context, and use this actionable information to both address the situation at hand and remediate gaps in your security posture.

Recover

Recover quickly. Recover deleted AD objects or just specific attributes in a few clicks, and restore entire domains or your whole forest to get your organization back in business quickly.









Modular and Integrated

Netwrix products are designed to be licensed and deployed separately. This approach enables organizations to mature their ITDR strategy at their own pace, while eliminating the headache of dealing with multiple vendors, contracts, licensing models, and — perhaps most important — support teams that tend to start pointing fingers at each other when a problem arises.

At the same time, it removes the risk of having a single point of failure in the form of a point solution that claims to cover all aspects of ITDR. Netwrix offers the safer and more dependable option of using a set of solutions that are each designed specifically to handle different aspects of ITDR.

Why Netwrix

- **Complete solutions** — Netwrix provides end-to-end solutions that not only address all NIST functions but cover all the key attack surfaces: identity, data and infrastructure. For example, Netwrix offers the industry's most complete solution for Active Directory.

Netwrix solutions	Data Access Governace	Identity Governance and Administration	Active Directory Security	Data Loss Prevention	Compliance	Privilege Access Management	Password Solutions
NIST Functions	Identify	Protect	Detect	Respond	Recover	Govern	
<div>  Unstructured Data  Structured Data  Directory  Cloud  Servers  Workstations  Devices  Applications </div>							

Netwrix solutions for today's tough cyber-challenges.

- **Fits your organization's needs** — Whether you're on premises, in the cloud or hybrid, and whether you're focused on protecting your infrastructure or credentials, we have solutions to fit your organization's needs.
- **Easy scalability** — Our open, scalable architecture meets the needs of organizations of any size and complexity, from SMBs to global enterprises.
- **Ecosystem integrations** — Maximize the value of your previous investments by integrating Netwrix solutions with your current IT and security tools.

About Netwrix

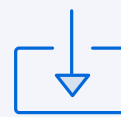
Netwrix champions cybersecurity to ensure a brighter digital future for any organization. Netwrix's innovative solutions safeguard data, identities, and infrastructure reducing both the risk and impact of a breach for more than 13,500 organizations across 100+ countries. Netwrix empowers security professionals to face digital threats with confidence by enabling them to identify and protect sensitive data as well as to detect, respond to, and recover from attacks.

For more information, visit www.netwrix.com

Next Steps



[Schedule a demo](#)



[Request quote](#)

CORPORATE HEADQUARTER:

6160 Warren Parkway, Suite
100 Frisco, TX, US 75034

PHONES:

1-949-407-5125
Toll-free (USA): 888-638-9749

OTHER LOCATIONS:

Spain:	+34 911 982608
Netherlands:	+31 858 887 804
Sweden:	+46 8 525 03487
Switzerland:	+41 43 508 3472
France:	+33 9 75 18 11 19
Germany:	+49 711 899 89 187
Hong Kong:	+852 5808 1306
Italy:	+39 02 947 53539

SOCIAL:



netwrix.com/social

5 New Street Square, London
EC4A 3TW

+44 (0) 203 588 3023