WHY NETWRIX

IDENTITY MANAGEMENT

- Quick Deployment and Low TCO
- Flexible Deployment Options
- Governance without Complexity

IDENTITY THREAT DETECTION AND RESPONSE

- Patented Innovation
- Complete Protection
- Flexible and scalable

DIRECTORY MANAGEMENT

- All-in-One Management
- Seamless Integration
- Rapid Deployment

PRIVILEGED ACCESS MANAGEMENT

- Zero Standing Privileges
- No Hidden Fees
- Rapid Time to Value

DATA SECURITY POSTURE MANAGEMENT

- Complete Visibility
- Cloud and On-Prem Support
- Flexible Deployment Options

ENDPOINT MANAGEMENT

- Multiple Deployment Options
- Multi-OS Coverage
- CIS Certified Templates

ABOUT NETWRIX

Netwrix is reinventing data security because traditional solutions fail if adversaries can exploit identities and escalate privileges. Netwrix starts by protecting identity, the #1 attack vector, and in parallel, classifies data, identifies risks, removes exposures, controls privilege, enforces data loss prevention (DLP) policies, blocks threats, and streamlines recovery to secure each organization's most valuable asset, their data.

Netwrix's comprehensive and extensible solutions for Identity Management, Identity Threat Detection and Response (ITDR), Privileged Access Management (PAM), Directory Management, Endpoint Management, and Data Security Posture Management (DSPM) provide defense-in-depth to over 13,500 organizations across 100+ countries. With support for natural language AI queries and conversational security insights, Netwrix makes it easier, faster, and more economical than ever for security and IT teams to investigate and remediate threats.

NOTES

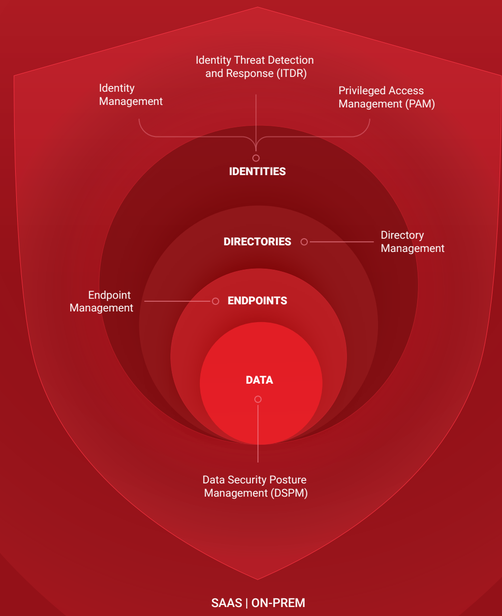
Corporate Headquarters:
6160 Warren Parkway, Suite 100
Frisco, TX, US 75034

Phone:
1-949-407-5125

Toll-free:
888-638-9749

netwrix

DATA SECURITY THAT STARTS WITH IDENTITY



SAAS | ON-PREM

IDENTITY MANAGEMENT

Netwrix Identity Management strengthens security, automates compliance, and streamlines user access management. It supports zero-trust governance, automates group and user lifecycle management, enforces strong password policies to reduce credential risks, and minimizes administrative overhead while ensuring timely, appropriate access.

- Identity Lifecycle and Workflows
- Group Lifecycle Management
- Entitlement Management
- Access Request Delegation
- Segregation of Duties
- Password Policy Enforcement
- Access Rights Certification
- Compliance Auditing and Reporting

DIRECTORY MANAGEMENT

Netwrix Directory Management enhances security and compliance with detailed auditing of on-premises and cloud directories, ensuring visibility into changes and access events. It streamlines user and group management through automation and delegation and enforces customizable password policies to reduce the compromise of weak or stolen credentials.

- Automated User and Group Management
- Change Auditing and Tracking
- Permission reviews and change tracking
- Password Policy Enforcement
- Group lifecycle Management
- User Self-Service

DATA SECURITY POSTURE MANAGEMENT (DSPM)

Netwrix Data Security Posture Management enables highly regulated organizations with complex, multi-cloud, and hybrid environments to easily discover and classify shadow data, assess, prioritize, and mitigate risks to their sensitive data, prevent data loss, and detect policy violations and suspicious behavior in time to prevent a data breach.

- Data Discovery and Classification
- Data Risk Assessment
- Data Exposure Remediation
- Data Access Visibility
- Compliance Capabilities
- Activity Monitoring and Threat Detection
- Data Lifecycle Management
- Endpoint Data Loss Prevention
- Incident Response Analysis

IDENTITY THREAT DETECTION AND RESPONSE (ITDR)

Netwrix Identity Threat Detection and Response (ITDR) empowers organizations to prevent breaches by eliminating risks before exploitation. It blocks unauthorized changes, enforces strong controls, and detects attacks in real time. Automated response and rapid AD forest recovery help security teams stop threats fast and keep businesses running.

- Identity security weaknesses
- Risk Remediation
- Threat Prevention
- Threat Detection
- Automated Threat Response
- Identity Attack Investigation
- Active Directory Change Remediation
- AD Forest Recovery

PRIVILEGED ACCESS MANAGEMENT (PAM)

Netwrix Privileged Access Management enforces Just-in-Time access and removes standing privileges. It discovers privileged accounts, provisions ephemeral access, and blocks lateral movement. With built-in Zero Trust controls like MFA, session recording, and access approvals, it secures systems across remote, hybrid, and on-prem environments.

- Privilege Discovery and Visualization
- Zero-Standing Privilege Provisioning
- VPN-less, Zero Trust Remote Access
- Endpoint Privilege Management
- Session Monitoring and Recording
- Compliance Reporting and Auditing
- Self Service Secure Access
- Vendor and Third-Party Access Controls

ENDPOINT MANAGEMENT

Netwrix provides complete endpoint configuration management, security, and compliance across multi-OS devices and environments. Its policy-based deployment framework prevents attacks and optimizes productivity across the endpoint lifecycle, including privilege management, peripheral device control, and application security.

- Endpoint Privilege Management
- Device Control and USB Encryption
- GPO Consolidation and Migration
- Compliance Validation and Monitoring
- Application Deployment and Security
- User Desktop Experience Management
- Browser and Application Network Security