netwrix

Data Security Posture Management (DSPM)

Discover and classify shadow data. Assess, prioritize, and mitigate risks to sensitive data, and detect threats in time to prevent a data breach

Netwrix DSPM enables highly regulated organizations with complex, multi-cloud, and hybrid environments to easily discover and classify shadow data, prevent its loss, monitor and analyze user activities, and detect suspicious behavior. This reduces the risk of data breaches and ensures compliance with regulatory requirements.

DISCOVER AND PROTECT SENSITIVE DATA

Discover and classify sensitive and regulated content across on-prem and cloud data repositories, tag it accurately to keep track of it, and uncover misconfigurations that traditional security tools miss.

AUTOMATICALLY ASSESS AND REMEDIATE RISKS

Analyze data security posture to detect misconfigurations, over -permissioned access, and compliance risks, prioritize the most pressing threats, and remediate them.

CONTINUOUSLY MONITOR CHANGES AND ALERT

Monitor activity and changes around sensitive data and alert on suspicious access patterns or anomalous data movements that could indicate account compromise or insider threats.

> “
>
> Even if you enforce least privilege and trust your employees as much as we do, you still need to know exactly who did what, when and where, so you can detect internal threats or hackers in time. You want to know that your sensitive data is safe — that is what Netwrix can tell me, and it is giving me peace of mind.
>
> John Bayes, IT Director, Hull College

Netwrix Auditor

- Windows File Servers
- SharePoint
- Oracle Database
- Exchange
- Windows Server

Netwrix Data Classification

- File Servers
- SharePoint
- Databases
- Exchange
- Tagging
- Remediation

Netwrix Access Analyzer

- File Systems
- Exchage
- Workflow Actions
- SharePoint
- FS Action
- SDD for UD
- Databases
- AD Action
- SDD for SD

Netwrix 1Secure DSPM

netwrix

Solve your most difficult data security challenges

DISCOVER AND CLASSIFY SENSITIVE DATA

Locate sensitive data within an organization and categorize it based on factors like confidentiality, sensitivity, and regulatory requirements. Enhance existing data loss prevention (DLP) solutions by accurately tagging sensitive data, enabling more precise DLP policy enforcement.

REMEDIATE DATA EXPOSURE

Don't just find data—automatically fix the issues that put it at risk, such as moving assets from insecure storage to secure environments, updating access permissions, or removing sensitive content.

MONITOR ACTIVITY AND DETECT THREATS

Track and analyze interactions to detect unusual or unauthorized access, insider threats, or compromised accounts. Automatically fix conditions that put sensitive data at risk, such as revoking excessive privileges, disabling users, or modifying group memberships.

MANAGE DATA THROUGHOUT ITS LIFECYCLE

Identify data types and their sensitivity levels, enabling the implementation of appropriate data retention, data archiving, and data deletion policies to ensure regulatory compliance and optimize data storage.

DATA RISK ASSESSMENT

Identify sensitive or high-risk data, evaluate vulnerabilities, such as misconfigurations or over-permissioned access, and strategically prioritize protective measures.

GET VISIBILITY INTO DATA ACCESS

Understand exactly who has access to what, how they are getting that access, and whether they are actually using it. Optimize access controls to uphold the principle of least privilege, ensuring each user has only the data access permissions necessary for their role.

MAKE COMPLIANCE EASY

Identify, classify, and manage data in line with evolving regulations to guarantee proper handling, storage, and protection of sensitive information. Implement structured processes for data privacy and governance, including periodic entitlement reviews and efficient responses to Data Subject Access Requests (DSARs).

PREVENT DATA LOSS AT REST AND IN MOTION

Content-aware protection prevents unauthorized data sharing and exfiltration through contextual scanning of emails, messaging apps, and USB devices. eDiscovery identifies sensitive data stored on endpoints for encryption or deletion, ensuring compliance with GDPR, HIPAA, PCI-DSS, and more.

WHY NETWRIX?

DEEP VISIBILITY INTO IDENTITY & DATA SECURITY

Netwrix solutions connect identity security and data risk management, making it easier to discover datasecurity threats and remediate risks through automation.

COMPREHENSIVE COVERAGE FOR CLOUD & ON-PREMISES DATA SECURIT

Govern access to structured or unstructured data, whether on-premises or across multi-cloud environments.

FLEXIBLE DEPLOYMENT OPTIONS

Choose the environment that best fits your organization—on-premises, virtual, hybrid or cloud-native. Scalable for security teams in small businesses and large enterprises.

Next Steps — REQUEST ONE-TO-ONE DEMO

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