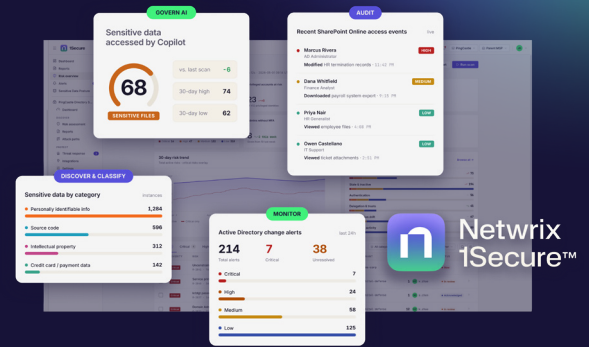


Netwrix 1Secure™

Daten schützen.
Identitäten absichern.
KI sicher einsetzen.



Netwrix 1Secure™ ist eine SaaS-Plattform, die Identity und Data Security vereint und damit Sicherheitslücken schließt, die zu Breaches und zur Offenlegung von Daten führen.

Innerhalb einer Stunde einsatzbereit und mit ersten Ergebnissen: Die Plattform erkennt sensible Daten, bewertet Identity-Risiken und identifiziert Bedrohungen in Hybrid Environments.

Mit kontinuierlichem Monitoring und einer auf KI ausgerichteten Governance reduziert 1Secure™ die Angriffsfläche, stärkt die Compliance und ermöglicht die sichere Einführung von Copilot.

Die wichtigsten Funktionen

Erkennung von Shadow Data und sensiblen Daten

Erkennen Sie übermäßig exponierte sensible Daten, erstellen Sie Berichte zu den damit verbundenen Aktivitäten und lassen Sie sich warnen, wenn jemand versucht, sich per Brute Force Zugriff auf sensible Datensätze zu verschaffen.

Erweiterte Risikobewertung

Führen Sie mehr als 210 Risikoprüfungen für Daten und Identity durch. Kombinieren Sie das branchenführende Assessment von PingCastle mit einer Datenrisikoanalyse, um das Risikoniveau Ihres Unternehmens systematisch zu senken.

KI-gestützte Risikobehandlung

Mit maßgeschneiderten, direkt umsetzbaren Empfehlungen zur Risikobehandlung von Netwrix AI reduzieren Sie Risiken in Ihrer hybriden Identity- und Datenumgebung schneller und effektiver.

Warnmeldungen bei kritischen Änderungen in Hybrid Environments

Sie werden umgehend über verdächtige Aktivitäten in Ihrer Umgebung informiert und können rechtzeitig reagieren, bevor ernsthafter Schaden entsteht. Fragen Sie Netwrix Neo, den in Netwrix 1Secure™ integrierten KI-Assistenten, was passiert ist, und erhalten Sie verständliche Empfehlungen zur Behebung.

Transparenz bei Berechtigungen

Erkennen Sie unbefugte Rechtheausweitungen und erhalten Sie alle relevanten Fakten zu Änderungen an Ihren Security Groups – einschließlich wer, was und wann. Lassen Sie sich warnen, wenn Berechtigungen mit hohem Risiko hinzugefügt werden, und identifizieren Sie übermäßig exponierte Daten.

Sensible Daten mit Sensitivity Labels schützen

Verhindern Sie Datenexfiltration und verbessern Sie Ihre Richtlinien zur Behebung von Datenrisiken, indem Sie sensible Daten mit Labels kennzeichnen. Erhöhen Sie die Transparenz, indem Sie erkennen, welche sensiblen Daten übermäßig weitreichend berechtigt sind und ob sensible Daten nicht gekennzeichnet wurden.

Vorteile



Risikobehaftete Daten identifizieren

Ermitteln Sie, wo sich PII-, PHI- und PCI-Daten befinden, erkennen Sie unzulässige Dateizugriffe und decken Sie fehlgeschlagene Zugriffsversuche auf, bevor Angreifer oder Auditoren sie entdecken.



Compliance Reports on demand erstellen

Verkürzen Sie die Audit-Vorbereitung von Wochen auf Sekunden – mit vorkonfigurierten Reports für HIPAA, DSGVO, PCI und SOX sowie Point-in-Time Snapshots, die Auditoren genau zeigen, was sich zu diesem Zeitpunkt geändert hat.



Erkennen, was M365 Copilot offenlegt

Erkennen Sie genau, welche sensiblen Daten Copilot wem zugänglich macht und welche übermäßigen Berechtigungen dabei übernommen werden. Überwachen Sie Copilot-Aktivitäten, damit Sie riskante Vorgänge erkennen, bevor daraus ein Breach entsteht.



In wenigen Minuten eingerichtet – Ergebnisse sofort verfügbar

Sparen Sie sich wochenlange Deployments und monatelange Wartezeiten. Netwrix 1Secure™ läuft in der Cloud, ohne dass Infrastruktur verwaltet werden muss, und liefert innerhalb weniger Minuten konkrete Erkenntnisse zu Risiken.



Mehr aus Ihrer Microsoft-Investition herausholen

Steigern Sie den Wert Ihrer Microsoft-Investition durch mehr Transparenz bei sensiblen Daten, einschließlich MIP Labels. Erkennen Sie, worauf Copilot zugreift und welche übermäßigen Berechtigungen dabei übernommen werden.



Risiken mithilfe von KI-Empfehlungen minimieren

Sie wissen genau, wie sich Probleme beheben lassen. KI-generierte Schritte zur Behebung zeigen Ihnen, wie Sie jedes Finding schließen – damit Ihr Team direkt handeln kann, statt erst nach dem richtigen Ansatz zu suchen.



Bedrohungen erkennen und untersuchen

See the full data-access story, not isolated events. Betrachten Sie sämtliche Datenzugriffe im Zusammenhang statt als isolierte Events. Das Alert Dashboard zeigt Zugriffe auf sensible Dateien, anonyme Freigaben, riskante Aktivitäten und die Offenlegung durch Copilot. Fragen Sie Neo, den in Netwrix 1Secure™ integrierten KI-Assistenten, was hinter einem Ausschlag steckt, und erhalten Sie innerhalb von Sekunden eine verständliche Antwort.



KI-Governance-Risiken zentral im Blick

Steuern Sie in einer zentralen Ansicht, worauf KI zugreifen kann. Sehen Sie die Gesamtzahl sensibler Dateien, frei zugängliche Daten, die Verteilung nach Datentyp in SharePoint und Windows sowie Benutzer mit auffälligen Zugriffstrends.

Unsere Pakete im Vergleich

Netwrix 1Secure™		
DATA	IDENTITY	★ AM BELIEBTESTEN COMPLETE
DATEN SCHÜTZEN UND COMPLIANCE NACHWEISEN	IDENTITY SCHÜTZEN UND COMPLIANCE NACHWEISEN	ALLES SCHÜTZEN UND COMPLIANCE NACHWEISEN
✓ PingCastle Risk Assessment (Dateneinblicke) ✓ KI-gestützte Empfehlungen zur Risikobehhebung ✓ Aktivitätsüberwachung und Warnmeldungen ✓ Netwrix Neo KI-Assistent ✓ Aktuelle Statusberichte Datenerkennung und -klassifizierung	✓ PingCastle Risk Assessment (Dateneinblicke) ✓ KI-gestützte Empfehlungen zur Risikobehhebung ✓ Aktivitätsüberwachung und Warnmeldungen ✓ Netwrix Neo KI-Assistent ✓ Aktuelle Statusberichte Datenerkennung und -klassifizierung	✓ PingCastle Risk Assessment (Dateneinblicke) ✓ KI-gestützte Empfehlungen zur Risikobehhebung ✓ Aktivitätsüberwachung und Warnmeldungen ✓ Netwrix Neo KI-Assistent ✓ Aktuelle Statusberichte ✓ Datenerkennung und -klassifizierung
UNTERSTÜTZTE DATENQUELLEN	UNTERSTÜTZTE DATENQUELLEN	UNTERSTÜTZTE DATENQUELLEN
- Active Directory - Entra ID ✓ Windows Server ✓ SharePoint Online ✓ Exchange Online ✓ Windows File Server ✓ SOL Server	✓ Active Directory ✓ Entra ID - Windows Server - SharePoint Online - Exchange Online - Windows File Server - SOL Server	✓ Active Directory ✓ Entra ID ✓ Windows Server ✓ SharePoint Online ✓ Exchange Online ✓ Windows File Server ✓ SOL Server

Was unterscheidet Netwrix 1Secure™?



Automatische Updates

Profitieren Sie jeden Monat sofort von neuen Produktfunktionen – ohne langwierige Upgrades, Paket-Downloads oder das Einspielen von Patches.



Einfache Integration in Ihren Tech Stack

Behalten Sie Ihre Business Workflows bei und bereichern Sie Ihre Systeme mit wertvollen Informationen an, indem Sie Netwrix 1Secure™ nahtlos in Ihre Professional Services Automation (PSA) Tools integrieren.



Authentifizierung per Single Sign-on

Vereinfachen Sie die Benutzerauthentifizierung, zentralisieren Sie die Zugriffskontrolle und unterstützen Sie Compliance durch die Ausrichtung an Enterprise Access Management Practices.



Schnelle Time-to-Value

Erkennen Sie die erste reale Exposition bereits am ersten Tag – nicht erst nach einem sechswöchigen Deployment. Die Cloud-Plattform indiziert Datenquellen direkt beim Verbinden und zeigt Risiken innerhalb weniger Minuten im Dashboard an.

Nächste Schritte



Kostenlose Testversion



Mehr erfahren



Kontakt aufnehmen

netwrix

Data security that starts with identity™



Copyright © Netwrix Corporation. Alle Rechte vorbehalten. Netwrix ist eine Marke der Netwrix Corporation und/oder einer oder mehrerer ihrer Tochtergesellschaften und kann beim U.S. Patent and Trademark Office sowie in anderen Ländern eingetragen sein. Alle anderen Marken und eingetragenen Marken sind Eigentum ihrer jeweiligen Inhaber.