

WELCHE VORTEILE BIETET NETWRIX?

IDENTITY MANAGEMENT



Netwrix Identity Management verringert den Zeitaufwand für IT-Routineaufgaben und die Zugriffsverwaltung. Zugleich werden wir über Änderungen benachrichtigt, sodass wir schnell reagieren können.

CIO eines Finanzdienstleisters

IDENTITY THREAT DETECTION AND RESPONSE



Ein hervorragendes Produkt mit Sicherheitsfunktionen, die andere Lösungen nicht bieten. Überwachung allein genügt nicht – Bedrohungen müssen abgewehrt werden. Lösungen anderer Anbieter senden lediglich Benachrichtigungen.

IT-Sicherheits- und Risikomanager einer Bank

DIRECTORY MANAGEMENT



Ohne Netwrix Directory Management wären wir verloren – keine andere Lösung bietet einen vergleichbaren Funktionsumfang, eine derart einfache Konfiguration und die Möglichkeit, jede Herausforderung zu bewältigen.

Bereich Infrastruktur und Betrieb einer Behörde

PRIVILEGED ACCESS MANAGEMENT



Netwrix ließ sich einfach installieren: Unsere Techniker hatten innerhalb eines Tages alles konfiguriert und brauchten nicht mehrere Wochen oder Unterstützung durch teure Berater wie bei anderen Lösungen.

IT Operations Manager eines Transport- und Logistikunternehmens

DATA SECURITY POSTURE MANAGEMENT



Auch bei Anwendung des Prinzips der geringsten Rechte müssen wir wissen, welche Benutzer wann und wo welche Aktivitäten durchgeführt haben. Mit Netwrix haben wir die Gewissheit, dass unsere Daten sicher sind.

IT-Leiter einer Bildungseinrichtung

ENDPOINT MANAGEMENT



Mit Netwrix Endpoint Policy Manager können wir die Auflagen des Bundes erfüllen. Ohne die Lösung wären wir nicht in der Lage, die erforderlichen Einstellungen sicher anzuwenden.

IT-Analyst einer Behörde

INFORMATIONEN ZU NETWRIX

Netwrix definiert Datensicherheit neu, da herkömmliche Lösungen keinen ausreichenden Schutz bieten, wenn Angreifer Identitäten ausnutzen und Berechtigungen ausweiten können. Für Netwrix beginnt Datensicherheit deshalb mit dem Schutz von Identitäten, dem zentralen Angriffsvektor. Parallel dazu ermöglichen Lösungen von Netwrix die Klassifizierung von Daten, Ermittlung von Risiken, Verringerung von Angriffsflächen, Kontrolle von Berechtigungen, Durchsetzung von Richtlinien zur Verhinderung von Datenverlust (DLP), Abwehr von Bedrohungen und Optimierung der Wiederherstellung, um die wertvollste Ressource von Unternehmen zu schützen: ihre Daten.

Mit den funktionsstarken und erweiterbaren Lösungen von Netwrix für die Identitätsverwaltung, Identity Threat Detection and Response (ITDR), Privileged Access Management (PAM), Verzeichnisverwaltung, die Verwaltung von Endgeräten und Data Security Posture Management (DSPM) profitieren mehr als 13.500 Unternehmen aus über 100 Ländern weltweit von umfassendem Schutz. Netwrix unterstützt KI-Anfragen in natürlicher Sprache und dialoggestützte Sicherheitsanalysen. Dadurch können Sicherheits- und IT-Teams Bedrohungen schneller, einfacher und kostengünstiger denn je untersuchen und abwehren.

NOTIZEN

 5 New Street Square,
London, EC4A 3TW, UK

 +49 221 599 88 029

 www.netwrix.de

netwrix

DATA SECURITY THAT STARTS WITH IDENTITY



IDENTITY MANAGEMENT

Netwrix Identity Management erhöht die Sicherheit, automatisiert die Compliance und vereinfacht die Verwaltung des Benutzerzugriffs. Die Lösung unterstützt Zero-Trust-Governance, automatisiert die Verwaltung des Gruppen- und Benutzerlebenszyklus und setzt Richtlinien für sichere Passwörter durch, um Risiken im Zusammenhang mit Anmeldeinformationen zu mindern. Sie verringert außerdem den Verwaltungsaufwand und stellt sicher, dass Benutzer jederzeit über die richtigen Zugriffsrechte verfügen.

- Identitätslebenszyklus und Workflows
- Verwaltung des Gruppenlebenszyklus
- Berechtigungsverwaltung
- Delegation der Zugriffsanforderung
- Aufgabentrennung
- Durchsetzung von Kennwortrichtlinien
- Zertifizierung von Zugriffsrechten
- Compliance-Audits und Berichterstellung

IDENTITY THREAT DETECTION AND RESPONSE (ITDR)

Mit Netwrix Identity Threat Detection and Response (ITDR) können Unternehmen Risiken beseitigen, bevor sie für Angriffe ausgenutzt werden, und so Datenschutzverletzungen vermeiden. Die Lösung wehrt Gefahren an der Quelle ab, setzt strenge Kontrollen durch und erkennt Angriffe in Echtzeit. Automatisierte Reaktionen und eine schnelle Wiederherstellung der AD-Gesamtstruktur ermöglichen es Sicherheitsteams, Bedrohungen schnell abzuwehren und den Geschäftsbetrieb aufrechtzuerhalten.

- Schwachstellen in der Identitätssicherheit
- Risikominderung
- Bedrohungsvermeidung
- Bedrohungserkennung
- Automatisierte Reaktion auf Bedrohungen
- Untersuchung von Angriffen auf Identitäten
- Aufhebung von Änderungen in Active Directory
- Wiederherstellung der AD-Gesamtstruktur

DIRECTORY MANAGEMENT

Netwrix Directory Management gewährt durch die detaillierte Überwachung von lokalen und cloudbasierten Verzeichnissen Einblick in Änderungen und Zugriffe und sorgt so für mehr Sicherheit und bessere Compliance. Die Lösung vereinfacht die Benutzer- und Gruppenverwaltung durch Automatisierung und Delegation und setzt individuell anpassbare Kennwortrichtlinien durch, um die Kompromittierung unsicherer oder gestohlener Anmeldeinformationen zu verhindern.

- Automatisierte Benutzer- und Gruppenverwaltung
- Überwachung und Nachverfolgung von Änderungen
- Zugriffsüberprüfungen und Überwachung von Berechtigungen
- Durchsetzung von Kennwortrichtlinien
- Verwaltung des Gruppenlebenszyklus
- Self-Services für Benutzer

PRIVILEGED ACCESS MANAGEMENT (PAM)

Netwrix Privileged Access Management setzt den Just-in-Time-Zugriff durch und macht permanente Berechtigungen überflüssig. Die Lösung identifiziert privilegierte Konten, stellt temporäre Zugriffsrechte bereit und verhindert laterale Bewegungen. Mit integrierten Zero-Trust-Kontrollen wie MFA, der Aufzeichnung von Sitzungen und der Genehmigung von Zugriffsrechten schützt sie Systeme in Remote-, hybriden und lokalen Umgebungen.

- Visualisierung von Berechtigungen
- Bereitstellung von Zero Standing Privileges
- Zero-Trust-Remote-Zugriff ohne VPN
- Verwaltung von Endgeräteberechtigungen
- Überwachung und Aufzeichnung von Sitzungen
- Compliance-Berichte und -Audits
- Sicherer Zugriff per Self-Service
- Kontrollen für den Zugriff von Lieferanten

DATA SECURITY POSTURE MANAGEMENT (DSPM)

Mit Netwrix Data Security Posture Management können Unternehmen mit komplexen, Multi-Cloud- und hybriden Umgebungen Schattendaten ganz einfach auffinden und klassifizieren, Risiken für ihre sensiblen Daten bewerten, priorisieren und mindern, Datenverlust verhindern und Richtlinienverstöße und verdächtiges Verhalten rechtzeitig erkennen, um Datenschutzverletzungen zu vermeiden.

- Auffinden und Klassifizieren von Daten
- Bewertung der Risiken für Daten
- Behebung von Datenproblemen
- Einblick in Datenzugriffe
- Compliance-Funktionen
- Überwachung von Aktivitäten und Bedrohungserkennung
- Verwaltung des Datenlebenszyklus
- Verhinderung von Datenverlust auf Endgeräten
- Analyse der Reaktion auf Vorfälle
- KI-gestützte Bedrohungsabwehr

ENDPOINT MANAGEMENT

Netwrix bietet umfassende Funktionen für die Verwaltung der Konfiguration, die Sicherheit und Compliance von Endgeräten für Geräte und Umgebungen mit mehreren Betriebssystemen. Das Framework für die richtlinienbasierte Bereitstellung sorgt dafür, dass Angriffe verhindert werden und die Produktivität über den gesamten Lebenszyklus von Endgeräten hinweg optimiert wird, einschließlich Berechtigungsverwaltung, Kontrolle von Peripheriegeräten und Anwendungssicherheit.

- Verwaltung von Endgeräteberechtigungen
- Gerätekontrolle und USB-Verschlüsselung
- Konsolidierung und Migration von Gruppenrichtlinienobjekten
- Überprüfung und Überwachung der Compliance
- Bereitstellung und Sicherheit von Anwendungen
- Verwaltung von Desktop-Oberflächen
- Kontrollierter Zugriff von Browsern und Anwendungen auf Netzwerkressourcen