netwrix

Data security that starts with identity™

Cybersecurity Lösungen

Erfahren Sie, wie die Lösungen von Netwrix Ihrem Unternehmen helfen können, morgen sicherer zu sein als heute, und Kosten zu sparen.

Cybersecurity Lösungen

(DSPM)

Data Security Posture Management

Identifizieren Sie sensible Daten und überwachen Sie die Aktivitäten der Benutzer, um verdächtiges Verhalten zu erkennen und so das Risiko von Datenlecks zu verringern.

Directory Management

Verwalten Sie Konten und Zugriffsrechte über Verzeichnisse hinweg mithilfe von Automatisierung, Transparenz und der Durchsetzung von Richtlinien.

(ITDR)

Identity Threat Detection & Response

Seien Sie Identitätsbedrohungen immer einen Schritt voraus – beheben Sie Risiken, blockieren Sie Bedrohungen, erkennen und reagieren Sie sofort und stellen Sie die Wiederherstellung Ihrer Identitätsinfrastruktur sicher.

Identity Management

Verwalten und steuern Sie Identitäten in großem Maßstab, indem Sie den Zugriff automatisieren, die Ausweitung von Berechtigungen eindämmen und die Einhaltung von Vorschriften vereinfachen.

Endpoint Management

Verhindern Sie Angriffe, optimieren Sie die Produktivität und stellen Sie die Einhaltung von Vorschriften auf Endgeräten mit verschiedenen Betriebssystemen in verteilten Umgebungen sicher.

Privileged Access Management

Schützen Sie kritische Systeme mit den Lösungen von Netwrix für die Verwaltung privilegierter Zugriffe. Sichern Sie Administratorkonten, setzen Sie das Prinzip der geringsten Berechtigungen durch und verhindern Sie den Missbrauch von Anmeldedaten.

Cybersecurity Lösungen

(DSPM)

Data Security Posture Management

Entdecken und klassifizieren Sie Schatten-Daten. Ermitteln Sie Risiken für sensible Daten, priorisieren Sie diese und mindern Sie sie, und erkennen Sie Bedrohungen rechtzeitig, um Datenlecks zu verhindern.

	Key Features	Produkte
Auditor	• Änderungsüberwachung • Compliance-Berichterstattung • Echtzeit-Warnmeldungen • Analyse des Benutzerverhaltens • Detaillierte Prüfpfade • Überwachung erweiterter Berechtigungen • Proaktive Erkennung von Bedrohungen • Zentrales Audit-Dashboard	Windows File Server, Nutanix, Dell EMC, SharePoint & Teams, NetApp, SQL Server, Synology, Oracle, Qumolo, Access Reviews
Data Classification	• Ermittlung sensibler Daten • Datenklassifizierung • Optische Zeichenerkennung • Inkrementelle Indizierung • Microsoft Purview Information Protection-Labels • Datenkennzeichnung • Auskunftsersuchen betroffener Personen	SQL Server, Dell EMC, PostgreSQL, Nutanix Files, Oracle, Qumulo, Windows File Server, SharePoint - Hybrid, NetApp, Exchange - Hybrid
Endpoint Protector	• Daten verschlüsseln und entschlüsseln • Manuelle oder automatische Scans • Daten löschen • Einhaltung gesetzlicher Vorschriften (DSGVO, HIPAA usw.) • Sperrliste für Scan-Standorte • Optische Zeichenerkennung • DLP für Drucker und USB-Geräte • Dateiname, Speicherort, vordefinierte Sperrliste usw.	**Content Aware Protection** For Windows, MacOS, and Linux Set Transfer limit within a specific time interval Dashboards, Reports, and Analysis **eDiscovery** For Windows, MacOS, and Linux Predefined content such as Credit Card, SSN, and many more
Access Analyzer	• Erkennung sensibler Daten • Einblicke in Dateiberechtigungen • Detaillierte Zugriffskontrolle • Analyse unstrukturierter Daten • Abwehr von Bedrohungen durch Entzug von Berechtigungen, Löschen nicht benötigter Konten, Deaktivieren unberechtigter Benutzerkonten und mehr.	File Systems, Sensitive Data Discovery for Unstructured Data, SharePoint - Hybrid, Exchange - Hybrid, Sensitive Data Discovery for Databases, Databases

Cybersecurity Lösungen

Directory Management

Vereinfachung und Sicherung der Verzeichnisverwaltung

	Key Features	Produkte
Auditor	• Änderungsüberwachung • Compliance-Berichte • Warnmeldungen zu Bedrohungsmustern • Detaillierte Prüfpfade • Berichte zu aktuellen Konfigurationen • Risikobewertung • Gruppenrichtlinien, erfolgreiche und fehlgeschlagene Anmeldungen, Berechtigungsberichte und mehr. • Nachverfolgung inaktiver Benutzer • Interaktive Suche • Warnmeldungen bei ablaufenden Passwörtern	**Active Directory** • Teilen Sie Passwörter, Schlüssel, Profile und andere vertrauliche Daten sicher mit Ihren Teamkollegen – und niemandem sonst. • Synchronisieren Sie Passwörter plattform- und geräteübergreifend, damit Nutzer von überall sicher darauf zugreifen können. • Jedes passwortbezogene Ereignis wird gespeichert, um den Anforderungen von Prüfern gerecht zu werden. • Rollenbasierte Zugriffskontrolle. • Einfache Verwaltung. • Starke Passwörter **Microsoft Entra ID** • Anmeldeaktivitäten bei Entra ID • Erstellte und gelöschte Benutzerkonten • Änderungen der Gruppenzugehörigkeit • Entra ID-Rollen und ihre Mitglieder
Directory Manager	• Identitätslebenszyklus-Management • Unterstützung für Zugriffsanfragen • Analysen und Berichterstellung • Richtlinien- und Rollenverwaltung • Automatisierte Bereitstellung • Self-Service-Passwortverwaltung • Berechtigungsverwaltung • Delegierte Benutzer- und Gruppenverwaltung • Protokollierung • Temporäre Mitgliedschaft	**Group Management** • Gruppenmitgliedschaft automatisch aktualisieren • Gruppenverwaltung delegieren • Gruppenverantwortliche zuweisen **Identity Management** • Benutzerverwaltung für AD und Entra ID • Automatisierung der Benutzeran- und -abmeldung **Password Management** • Passwort zurücksetzen mit MFA • Single Sign-On aktiviert
Password Policy Enforcer	• Wenden Sie bis zu 256 Richtlinien für lokale und Domänenpasswörter auf Benutzer, Domänengruppen und Organisationseinheiten an. • Erweiterte Regeln zur Passwortkomplexität • Überprüfung von Passwörtern anhand von Datenbanken mit kompromittierten Anmeldedaten • Detaillierte Anpassung der Richtlinien • Gewährleistung der Einhaltung verschiedener regulatorischer Rahmenwerke, darunter CIS, HIPAA, NERC CIP, NIST 800-63B und PCI DSS.	**Password Policy Enforcer** • Verhindern Sie Passwörter, die Sie als schwach erachten, mithilfe einer Wörterbuchregel, mit der Sie die Erkennung von Nicht-Alphabetzeichen, die Erkennung von Ersetzungen, die bidirektionale Analyse, die Wildcard-Analyse und die Übereinstimmungstoleranz steuern können • Erhöhen Sie die Sicherheit, indem Sie prüfen, ob Passwörter bei früheren Sicherheitsverletzungen offengelegt wurden • Erstellen Sie genau die Richtlinien, die Sie benötigen, indem Sie aus über 20 hochgradig anpassbaren Regeln auswählen

Cybersecurity Lösungen

Identity Threat Detection & Response

Behalten Sie die Oberhand über Identitätsbedrohungen durch proaktive Prävention, Erkennung und Abwehr von Bedrohungen in Echtzeit sowie schnelle Wiederherstellung, um die Geschäftskontinuität sicherzustellen.

	Key Features	Produkte
PingCastle	• Sicherheitslücken schneller erkennen, um Abhilfemaßnahmen zügiger umzusetzen und die Sicherheitslage zu verbessern • Überblick über den Gesamtzustand von AD und Entra ID anhand von 150 Sicherheitsprüfungen • Zuordnung zu Frameworks • Anleitungen zur Behebung von Problemen • Maßgeschneiderte Berichte mit Fokus auf kritische Befunde	**PingCastle Enterprise** • Setzen Sie eine detaillierte Zugriffskontrolle für mehr Sicherheit durch, indem Sie Benutzern bestimmte Rollen und Berechtigungen zuweisen • Historische Daten und Trendanalysen • Ermitteln Sie den Reifegrad Ihrer AD-Sicherheit anhand einer 20-Punkte-Bewertung in fünf Schlüsselbereichen: Domäne, Eigentumsverhältnisse, externe Vertrauensstellungen, interne Vertrauensstellungen und Risikobewertung • Geplante Scans
Threat Manager	• Erkennung und Reaktion auf spezifische Angriffstaktiken, darunter adminSDHolder, ACL-Manipulation, DCShadow, DCSync, Golden Ticket, Impossible Travel und andere. • Anormales Verhalten und Sicherheitsvorfälle • Täuschung von Bedrohungen • Untersuchung und Berichterstellung	**Threat Manager for Active Directory** • Verhinderung riskanter AD-Änderungen • Maschinelles Lernen und Analyse des Nutzerverhaltens **Threat Manager for Microsoft Entra ID** • Integration mit anderen Sicherheitstechnologien • Echtzeit-Benachrichtigungen
Access Analyzer	• Benutzer freischalten / Benutzerkennwort zurücksetzen • Objekte verschieben / Benutzer deaktivieren/aktivieren • Benutzer und Gruppen erstellen und SID-Verlauf löschen/festlegen • Computer deaktivieren/aktivieren • Erkennung von Shadow-Zugriffen	**Active Directory Action Module** • Änderungen an Active Directory vornehmen, z. B. Objekte löschen, Benutzer anlegen und die Gruppenzugehörigkeit ändern **Active Directory Permissions Analyzer** • Analyse der AD-Objektberechtigungen • Bewertung von Sicherheitslücken und Bedrohungen im Zusammenhang mit AD-Berechtigungen
Recovery for Active Directory	• Wiederherstellung und Rollback von AD-Attributen • Wiederherstellung gelöschter AD-Objekte • Unterstützung mehrerer Domänen • Unterstützung rollenbasierter Zugriffsrechte • E-Mail-Benachrichtigungen • Automatisierte Wiederherstellung der AD-Gesamtstruktur • Zurücksetzen einer AD-Domäne in einen früheren Zustand, wobei alle seit diesem Zeitpunkt vorgenommenen Änderungen rückgängig gemacht werden.	**Recovery for Active Directory** • Schützen Sie Ihr Active Directory, indem Sie ein schnelles Zurücksetzen von Objekten, Attributen und weiteren Elementen auf einen bekanntermaßen fehlerfreien Zustand ermöglichen – und das ohne Ausfallzeiten. Diese Lösung deckt alles ab, von AD-Objekten und Gruppenmitgliedschaften bis hin zu DNS-Einträgen und GPOs, und überwindet damit die Einschränkungen des AD-Papierkorbs.

Cybersecurity Lösungen

Identity Management

Sichern Sie jede Identität, optimieren Sie jeden Prozess und bleiben Sie den Compliance-Anforderungen immer einen Schritt voraus – ohne die Komplexität zu erhöhen.

	Key Features	Produkte
Identity Manager	• Manage Join, Move, and Leave Workflows • Access Request and Approval workflows • Policy and Role Management • Verify access rights across different applica-tions, roles, and user • populations, ensuring ongoing complianc Analytics and reporting • Out-of-the-box Workflows for Access Request	**Identity Manager Enterprise** • Enthält CyberArk-Konnektor • Enthält Concur-Konnektor • Enthält Easyvista-Konnektor • Enthält IBM-Konnektor • Enthält Qradar-Konnektor • Enthält SAP-Konnektor • Enthält ServiceNow-Konnektor
Directory Manager	• Identity Life Cycle Management • Support for Access Request • Analytics and Reporting • Policy and Role Management • Automated Provisioning • Self-Service Password Management • Entitlement Management • Delegated User and Group Management • Auditing • Temporary Memberships	**Group Management** • Gruppenmitgliedschaft automatisch aktualisieren • Gruppenverwaltung delegieren • Gruppenverantwortliche zuweisen • Benutzerverwaltung für AD und Entra ID • Automatisierung der Benutzeran- und -abmeldung **Password Management** • Passwort zurücksetzen mit MFA • Single Sign-On aktiviert
Password Policy Enforcer	• Wenden Sie bis zu 256 Richtlinien für lokale und Domänenpasswörter auf Benutzer, Domänengruppen und Organisationseinheiten an. • Erweiterte Regeln zur Passwortkomplexität • Überprüfung von Passwörtern anhand von Datenbanken mit kompromittierten Anmelde-daten • Detaillierte Anpassung der Richtlinien • Gewährleistung der Einhaltung verschiedener regulatorischer Rahmenwerke, darunter CIS, HIPAA, NERC CIP, NIST 800-63B und PCI DSS.	**Password Policy Enforcer** • Verhindern Sie Passwörter, die Sie als schwach erachten, mithilfe einer Wörterbuchregel, mit der Sie die Erkennung von Nicht-Alphabetscharakteren, die Erkennung von Ersetzungen, die bidirektionale Analyse, die Wildcard-Analyse und die Übereinstimmungstoleranz steuern können • Erhöhen Sie die Sicherheit, indem Sie prüfen, ob Passwörter bei früheren Sicherheitsverletzungen offengelegt wurden • rstellen Sie genau die Richtlinien, die Sie benötigen, indem Sie aus über 20 hochgradig anpassbaren Regeln auswählen

Cybersecurity Lösungen

Endpoint Management

Optimieren Sie die Konfiguration, Sicherheit und Compliance-Verwaltung von Endgeräten überall.

	Key Features	Produkte
Endpoint Protector	• Geräterechte können global, gruppenweise, pro Computer, Benutzer und Gerät konfiguriert werden. • Geräterechte festlegen – Verweigern, Zulassen, Nur-Lese-Zugriff usw. • Richtlinien für Zeiten außerhalb der Geschäftszeiten • Alle Dateiübertragungen und -versuche protokollierenUSB-Verschlüsselung erzwingen • Komplexe Master- und Benutzerkennwörter • Kennwortverwaltung und Fernlöschung	**Device Control** • Für Windows, macOS und Linux • USB-Sticks, Drucker, Bluetooth-Geräte, CD- und DVD-Laufwerke, externe Festplatten, Webcams, WLAN, Netzwerkfreigaben, iPhones, iPads, iPods, Kartenlesegeräte, Android-Smartphones und vieles mehr. **EasyLock Enforced Encryption** • Für Windows und macOS • 256-Bit-Verschlüsselung nach Militärstandard, Manipulationsschutz, zentralisierte Passwortverwaltung, Fernlöschung und vieles mehr.
Endpoint Policy Manager	• Verhindern Sie Malware-Infektionen und Datenverluste durch strenge Kontrolle der Nutzung von USB-, CD-ROM- und DVD-Geräten. • Anwendungskontrolle • Erstellen Sie Baseline-Profile und validieren Sie Ihre GPOs in großem Maßstab • Verwalten und sichern Sie virtuelle Desktops • Beenden Sie die GPO-Wildwucherung, um Ihre Windows-Umgebung übersichtlicher, einfacher zu verwalten und sicherer zu machen.	Removeable Device Management Application Delivery and Patching Windows 10 & 11 Management Desktop Automation Group Policy Compliance Group Policy Management Application, Browser and Java Security Microsoft Intune Management
Change Tracker	• Überwachung der Endpunktkonfiguration in Echtzeit • Automatisierte Workflow-Routinen zur Durchsetzung von Richtlinien • Module zur Erkennung von Konfigurationsabweichungen • Berichterstellung zum Compliance-Prüfpfad • Sofortige Benachrichtigungen bei unbefugten Änderungen • Prozess zum Management von Vorfällen	Windows Databases Linux Containers Cloud MacOS Unix Network Devices Virtualized Systems Industrial Control

Cybersecurity Lösungen

Privileged Access Management

Verhindern Sie Sicherheitsverletzungen, bevor sie entstehen. Sichern Sie privilegierten Zugriff.

	Key Features	Produkte
Privilege Secure	• Keine Standardberechtigungen • Just-in-Time-Zugriff • Intelligente Sitzungsaufzeichnung • Multi-Faktor-Authentifizierung • Sitzungen in Echtzeit steuern • Schutz von Dienstkonten • Einfache Beantwortung von Fragen der Rechnungsprüfer • Zugriff auf vorgefertigte und benutzerdefinierte Berichte	**Privilege Secure for Discovery** • Überprüfen Sie Ihr Netzwerk kontinuierlich, um alle privilegierten Konten zu identifizieren, damit kein Konto übersehen wird und potenzielle Sicherheitslücken beseitigt werden **Privilege Secure for Access Management** • Führen Sie ein aktuelles Verzeichnis aller privilegierten Konten • Verbieten Sie Administratoren die gemeinsame Nutzung von Konten • Reduzieren Sie die Anzahl der privilegierten Konten auf ein Minimum • Überwachen und protokollieren Sie alle privilegierten Aktivitäten
Endpoint Privilege Manager	• Erweitern Sie die Rechte von Standardbenutzern, sodass diese nur die Apps, MSI-Pakete, Betriebssystemprozesse, Applets und Skripte installieren oder ausführen können, die sie für ihre Arbeit benötigen. • Ereignisprotokollierung • Individuell anpassbare Eingabeaufforderungen • Für lokale Bereitstellung, MDM und Cloud geeignet • Bietet Benutzern die Möglichkeit, Anwendungen als Standardbenutzer oder mit erweiterten Rechten auszuführen	**Endpoint Privilege Manager** • Benutzerendgeräte • Beschränkung des Zugriffs auf Informationen • Sichere Authentifizierung • Löschung von Informationen • Protokollierung • Überwachung von Aktivitäten • Installation von Software auf Betriebssystemen • Trennung von Netzwerken • Anforderungen an die Anwendungssicherheit • Schutz von Informationssystemen während eines Audits
Password Secure	• Teilen Sie Passwörter, Schlüssel, Profile und andere vertrauliche Daten sicher mit Ihren Teamkollegen – und niemandem sonst. • Synchronisieren Sie Passwörter plattform- und geräteübergreifend, damit Nutzer von überall sicher darauf zugreifen können. • Jedes passwortbezogene Ereignis wird gespeichert, um den Anforderungen von Prüfern gerecht zu werden. • Rollenbasierte Zugriffskontrolle. • Einfache Verwaltung. • Starke Passwörter	**Password Secure** • Automatische Bereinigung • Passwort zurücksetzen • Unterstützung für Android und iOS • sswortlose Anmeldung • Multi-Faktor-Authentifizierung • Sitzungsverwaltung • Berichte • Passwortmaskierung • Passwortrichtlinien • Benutzerbeschränkungen und mehr

Über Netwrix

Netwrix setzt sich für Cybersicherheit ein, um jedem Unternehmen eine bessere digitale Zukunft zu sichern. Die innovativen Lösungen von Netwrix schützen Daten, Identitäten und Infrastruktur und verringern so sowohl das Risiko als auch die Folgen von Sicherheitsverletzungen für mehr als 13.500 Unternehmen in über 100 Ländern. Netwrix versetzt Sicherheitsexperten in die Lage, digitalen Bedrohungen selbstbewusst zu begegnen, indem es ihnen ermöglicht, sensible Daten zu identifizieren und zu schützen sowie Angriffe zu erkennen, darauf zu reagieren und die Folgen zu beheben.

wws.sysob.com/hersteller/netwrix

Wie geht es weiter`?

Sind Sie bereit, Microsoft Copilot sicher einzuführen und
das Risiko von Datenlecks nach der Einführung zu verringern?

Request a One-to-One Demo

Netwrix Unternehmenszentrale: 6160 Warren Parkway Suite 100, Frisco, TX, US 75034
Phone: 1-949-407-5125 Toll-free: 888-638-9749 EMEA: +44 (0) 203-588-3023 netwrix.com/social