SECURITY SUMMIT

Security Summit

Milano 11-12-13 marzo 2025

Clusit 25 2000-2025

ASTREA

netwrix

ITDR: Oltre il Prodotto

cips

Un Processo Essenziale per la Sicurezza delle Identità Digitali (E No...Non Parleremo di AI!)

Maurizio Taglioretti

Regional Manager SEEUR

Netwrix

Fabio Pelargonio

Presales Engineer

Netwrix

Veronica Conti

Sales Engineer

CIPS Informatica

Relatori

Maurizio Taglioretti

Regional Manager SEEUR, Netwrix

Appassionato di audit, compliance e sicurezza IT.

Veronica Conti

Sales Engineer, CIPS INFORMATICA

Professionista ed appassionata di sicurezza informatica con oltre15 anni di esperienza

Fabio Pelargonio

Presales Engineer, Netwrix

Professionista ed appassionato di sicurezza informatica con oltre 25 anni di esperienza.
CNE, ITIL v4 ,Prince2 Practitioner

Socio di: CHAPTERS

it.linkedin.com/in/tagliorettimaurizio

maurizio.taglioretti@netwrix.com

@mtaglior

https://www.linkedin.com/in/veronica-conti

veronica.conti@cips.it

it.linkedin.com/in/fabiopelargonio

fabio.pelargonio@netwrix.com

Active Directory Security/ITDR– I Problemi

L'IDENTITÀ È UN VETTORE DI ATTACCO

LE MINACCE ALL'IDENTITÀ POSSONO BYPASSARE I CONTROLLI IAM

IL CONTROLLO E LA VISIBILITÀ LIMITATI SU AD AUMENTANO IL RISCHIO

IL PASSAGGIO AL CLOUD HA AMPLIFICATO LA SFIDA DELLA SICUREZZA DELLE IDENTITÀ

verizon

"Secondo il Data Breach Investigation Report 2024 di Verizon nell'ultimo anno, il 45% delle violazioni dei dati è iniziato con un attacco basato sulle credenziali."

netwrix

ITDR (Identity Threat Detection and Response)

Nel contesto della sicurezza informatica in continua evoluzione, la protezione delle identità è diventata una priorità assoluta. Gli attacchi informatici sono sempre più sofisticati e mirano spesso a compromettere credenziali e identità degli utenti.
In questo scenario, **l'ITDR (Identity Threat Detection and Response)** si afferma come una **soluzione fondamentale** per individuare e contrastare le minacce che sfruttano le identità.

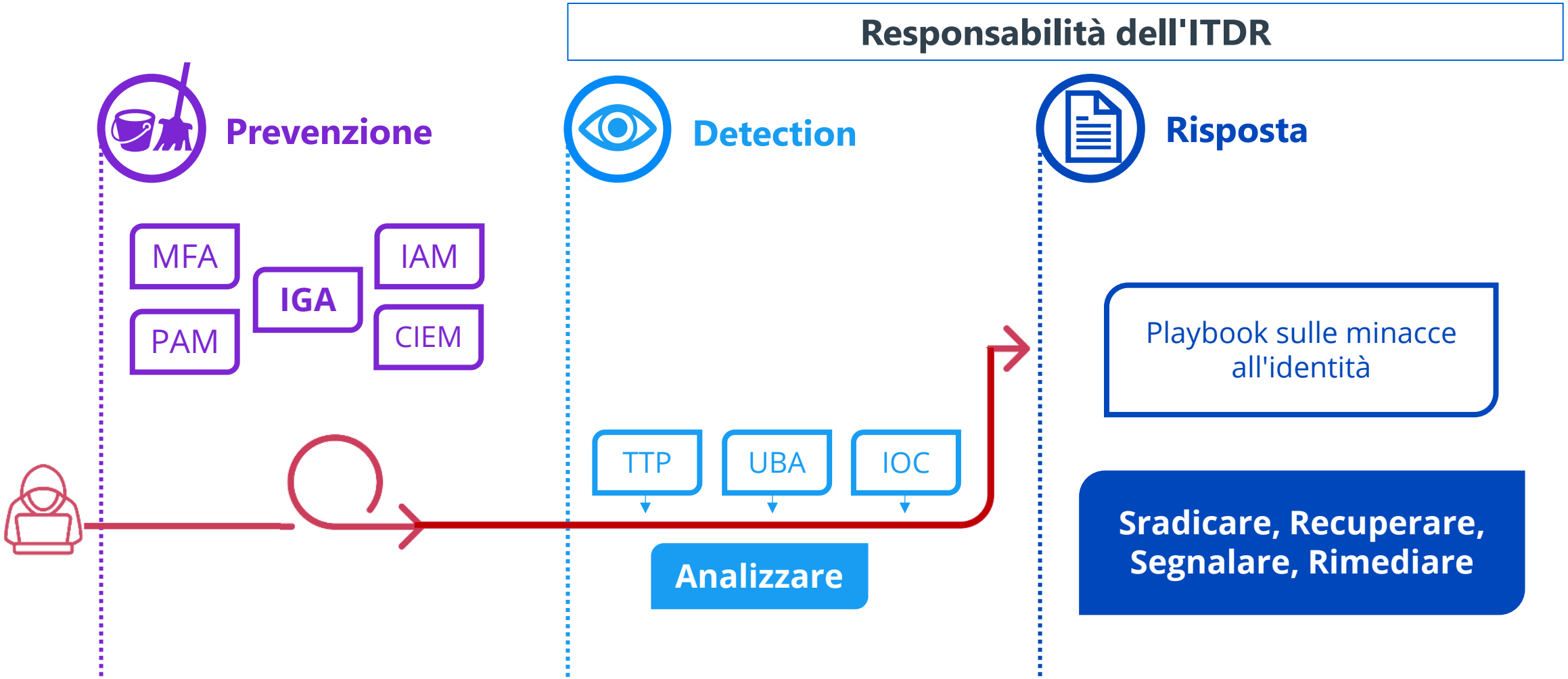
L'ITDR è un approccio di sicurezza progettato per rilevare e rispondere alle minacce che prendono di mira le identità.

A differenza di altre soluzioni come **EDR (Endpoint Detection and Response) e XDR (Extended Detection and Response),** che si concentrano rispettivamente sugli endpoint e su una visione più ampia della rete, l'ITDR si focalizza specificamente sulla **protezione delle identità digitali.**

Che cos'è l'ITDR? (Identity Threat Detection and Response) ?

- **Rilevamento e risposta alle minacce all'identità.**
- Dal 2022 **Gartner** utilizza il termine "Identity Threat Detection and Response" (ITDR) per descrivere un **insieme di strumenti e processi per la difesa dell'identità** e dei sistemi di protezione dell'identità.
- Allo stesso modo in cui si proteggono le infrastrutture, i dispositivi o le applicazioni, **ci si aspetta lo stesso livello di protezione per le identità.**
- L'ITDR è un importante complemento ai sistemi IAM perché **estende il framework IAM per controllare e monitorare l'accesso alle informazioni e ai sistemi sensibili.**

Gestione e protezione dell'identità



netwrix

Qualche cifra

- **98%** delle aziende ha visto un forte aumento del numero di identità
- Per ogni identità "umana" ci sono in media **45** Identità di macchine o servizi
- **74%** delle violazioni include un "elemento umano«
- **68%** delle aziende ha subito un impatto diretto sul business a seguito di una violazione dell'identità

Sources : Gartner & Verizon DBIR Report 2023

netwrix

Perché l'ITDR è essenziale?

- **Protezione delle identità**

Le identità digitali sono il nuovo perimetro di sicurezza e gli attacchi basati sulle credenziali sono in costante aumento. L'ITDR aiuta a **rilevare e prevenire l'uso improprio** delle identità, riducendo il rischio di accessi non autorizzati e violazioni di dati.

- **Integrazione con EDR e XDR**

L'ITDR non sostituisce EDR e XDR, ma li **complementa**, offrendo una visione più completa della sicurezza. Mentre EDR e XDR si focalizzano sulle minacce a livello di endpoint e rete, l'ITDR si occupa delle minacce **legate all'identità**.

- **Riduzione del rischio di movimenti laterali**

Gli aggressori utilizzano spesso credenziali compromesse per **spostarsi lateralmente** nella rete e accedere a dati sensibili. L'ITDR aiuta a **individuare e bloccare** questi movimenti, limitando l'impatto di una violazione.

- **Miglioramento della postura di sicurezza**

Implementando soluzioni ITDR, le aziende possono **rafforzare la loro strategia di sicurezza**, riducendo il rischio di attacchi e migliorando la capacità di risposta agli incidenti.

L'ITDR nelle vostre directory? Affidati all'approccio NIST

01
IDENTIFY

Identifica analizza e assegna priorità alle lacune di sicurezza nel tuo AD ed Entra ID in modo da poterle colmare prima che gli aggressori le sfruttino per rubare i tuoi dati.

02
PROTECT

Proteggi l'infrastruttura dell'identità correggendo i rischi identificati, applicando password complesse e implementando criteri di blocco per prevenire in modo proattivo le modifiche non autorizzate prima che diventino minacce alla sicurezza.

03
DETECT & RESPOND

Rileva in tempo anche gli attacchi avanzati basati sull'identità per prevenire una violazione.
Rispondi rapidamente alle minacce con opzioni di risposta automatizzate per un contenimento istantaneo.

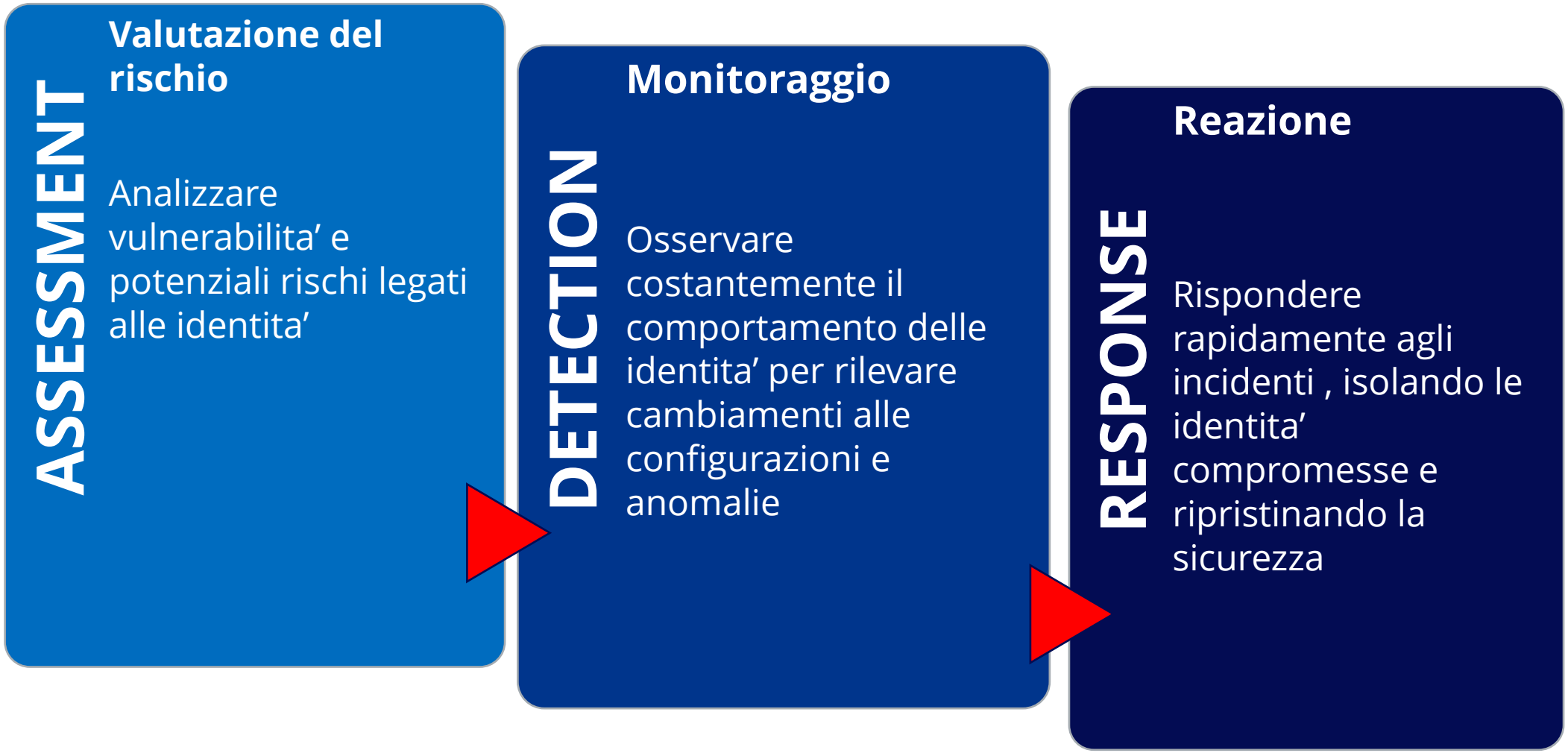
04
RECOVER

Ripristino dei sistemi critici. Esegui facilmente il rollback e il ripristino fino al ripristino completo della foresta.
Analizza il modo in cui si è verificato un incidente di sicurezza e utilizza le lezioni apprese per rinforzare le tue difese future.

05
GOVERN

Gestisci il tuo AD ibrido in modo che non sfugga al controllo in futuro. Automatizza la gestione di utenti e gruppi e semplifica le policy di sincronizzazione di AD.

Come implementare l'ITDR?



netwrix

Assessment e Valutazione del Rischio

Netwrix Ping Castle

netwrix

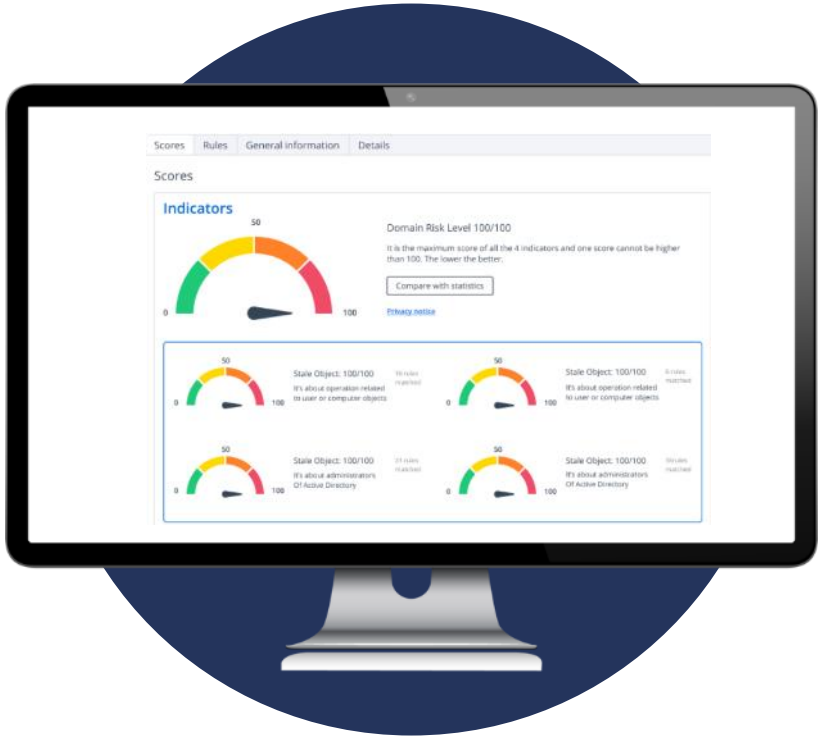
Netwrix PingCastle

Identificare e correggere i rischi nell'AD ibrido migliorando la postura di sicurezza

Identifica rapidamente i rischi
Ottieni una visione completa dei rischi in AD ed Entra ID. Sfrutta le mappature MITRE, ATT&CK™ e ANSSI con il punteggio di rischio per concentrare gli sforzi di sicurezza in modo efficace.

Colma le lacune di sicurezza
Riduci la superficie di attacco di Active Directory implementando strategie di correzione mirate. Segui i nostri consigli passo dopo passo, affrontando prima le vulnerabilità ad alto rischio per rafforzare il tuo livello di sicurezza dell'identità.

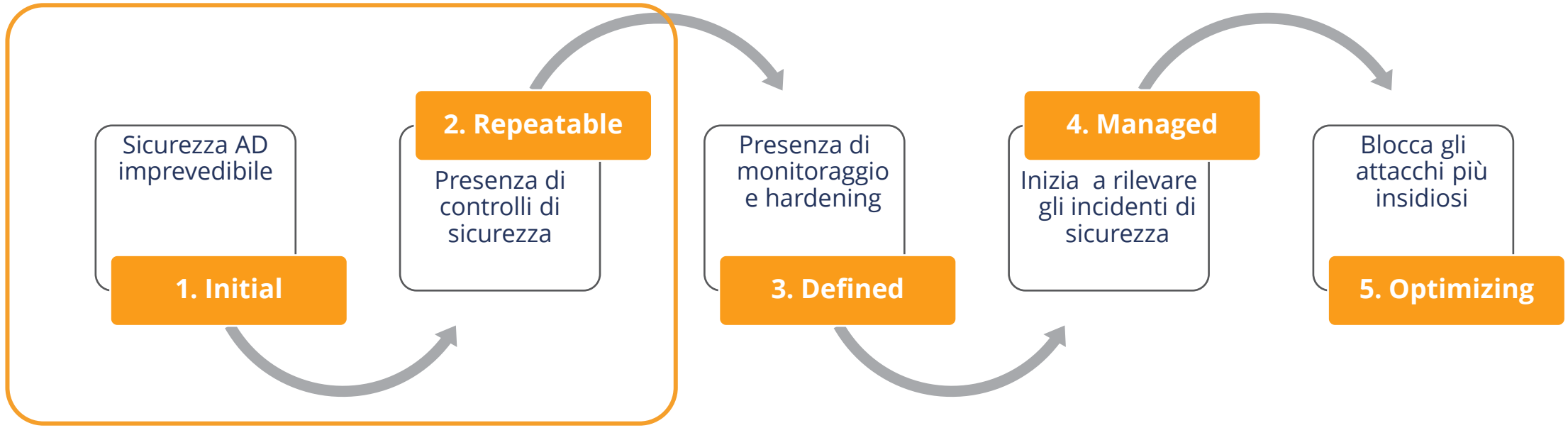
Monitora e migliora
Esegui Netwrix PingCastle su base pianificata su più domini per rilevare nuovi rischi e trust. Tieni traccia dei progressi e dei miglioramenti del punteggio di sicurezza per garantire una protezione AD continua.



La metodologia CMMI

Capability **M**aturity **M**odel **I**ntegration

Una metodologia sviluppata da **Carnegie Mellon University**, che ha anche progettato e sviluppato il CERT



FEATURES

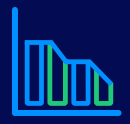
NETWRIX PINGCASTLE

Report di AD Health Check

Risk Assessment

Indicazioni di Risk Remediation

Valutazione del livello di maturità della sicurezza AD



Dati storici e analisi dei trend

AD Map

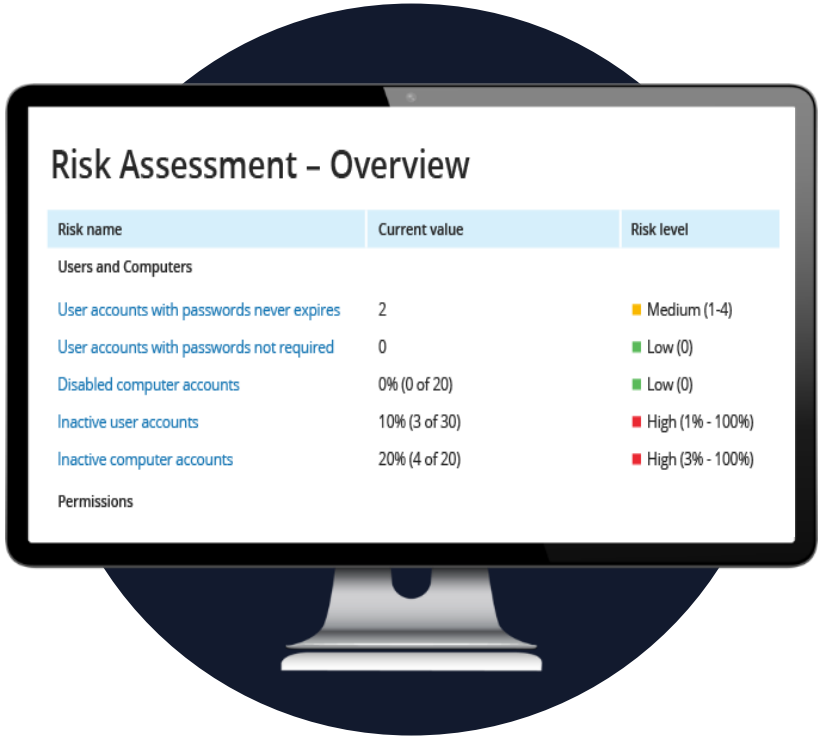
Detection e monitoraggio continuo

Netwrix Auditor

Netwrix Auditor

Identifica i rischi IT, rileva le attività sospette e indaga sugli incidenti di sicurezza

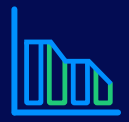
- Riduci al minimo il rischio di violazioni dei dati
- Raggiungi e dimostra la compliance
- Aumenta la produttività dei tuoi team IT



FEATURES

NETWRIX AUDITOR

Modifiche, Accessi, e analisi delle configurazioni



Risk Assessment

Alert in tempo reale sui modelli di minaccia

Verifiche dell'accesso degli utenti

Individuazione di comportamenti anomali

Rilevamento e classificazione dei dati sensibili (richiede NDC)

Report di compliance pronti all'uso

Ricerca simile a Google

netwrix

Prevention e risposta

Netwrix Threat Manager

netwrix

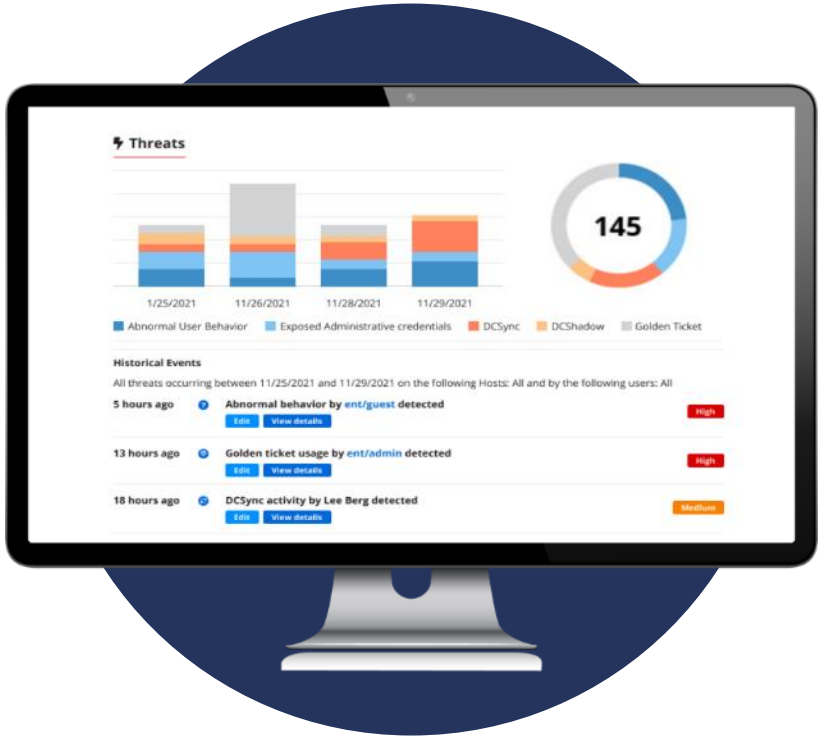
Netwrix Threat Manager

Rileva gli attacchi avanzati in corso e chiudili in un lampo

Blocca le minacce prima che si trasformino in violazioni. Rileva attacchi complessi e minacce interne in corso utilizzando l'apprendimento automatico e l'analisi del comportamento degli utenti.

Rispondi più velocemente di quanto umanamente possibile.
Contrasta le tecniche di attacco note alla velocità della luce sfruttando un catalogo di azioni di risposta automatizzate.

Semplifica l'indagine e il ripristino.
Ottieni informazioni complete su un incidente per consentire un ripristino tempestivo e informare la tua strategia di difesa.



NETWRIX THREAT MANAGER

Real-time Alerting

Risposta automatizzata alle minacce

Machine Learning e User Behavior Analytics (UBA)

Deception Tools

Contextual Risk Adjustment

Indagini complete

Minacce personalizzate

Integrazione con altre tecnologie di sicurezza

netwrix

Sicurezza AD unificata

Uso improprio dell'account privilegiato	Autorizzazioni eccessive	Problemi con la password	Account utente non aggiornati	Problemi relativi ai criteri di gruppo
Privilege Secure gestisce l'accesso degli account privilegiati e monitora le sessioni privilegiate	**GroupID** fornisce l'analisi e la pulizia dell'appartenenza ai gruppi per ridurre le autorizzazioni eccessive	**Netwrix Password Policy Enforcer** aiuta a far rispettare criteri di password complesse	**GroupID** automatizza l'identificazione e la gestione degli account utente inattivi e della loro appartenenza ai gruppi	**Auditor** genera report e avvisi sulle modifiche apportate a Criteri di gruppo
Auditor/Threat Manager monitorare e avvisa sulle attività degli utenti con privilegi	**Enterprise Auditor** fornisce un'analisi completa dei diritti di accesso e pulisce le autorizzazioni eccessive	**Enterprise Auditor** Fornisce report dettagliati sui problemi di sicurezza delle password	**Enterprise Auditor** pulisce gli oggetti utente AD obsoleti e non necessari in blocco e su larga scala	**Threat Prevention** Monitora e, facoltativamente, blocca le modifiche ai Criteri di gruppo

netwrix

Le nostre Soluzioni

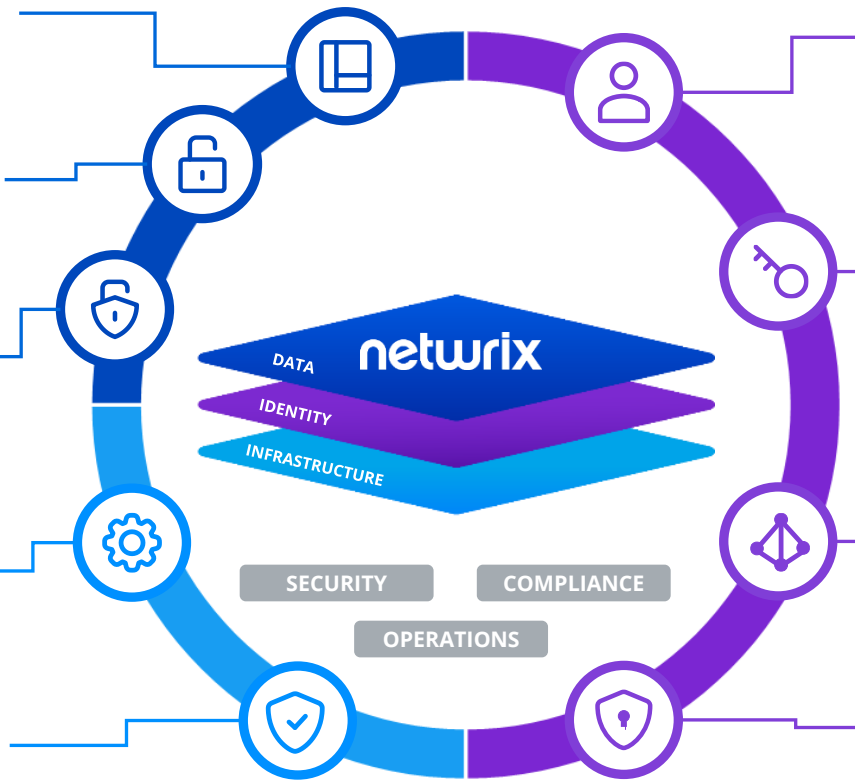
DATA DISCOVERY & CLASSIFICATION
Individua e classifica i dati sensibili non strutturati e strutturati ovunque si trovino

DATA ACCESS GOVERNANCE / DSPM
Allinea i diritti di accesso ai dati con i principi dei privilegi minimi per i dati strutturati e non strutturati

DATA LOSS PREVENTION
Scopri, monitora e proteggi i dati sensibili da fughe di notizie involontarie e dannose su tutti gli endpoint Windows, Mac e Linux

SECURITY CONFIGURATION MANAGEMENT
Mitigare i rischi operativi e di sicurezza attraverso l'identificazione proattiva delle deviazioni della configurazione

ENDPOINT MANAGEMENT & SECURITY
Configura, distribuisci e controlla facilmente le policy e lo spostamento dei dati da/verso gli endpoint utente multi-OS, applicando al contempo i privilegi minimi



IDENTITY GOVERNANCE & ADMINISTRATION
Provisioning, deprovisioning e gestione dei diritti acquisiti in modo accurato e tempestivo

PRIVILEGED ACCESS MANAGEMENT
Raggiungi l'obiettivo Zero Standing Privilege con un approccio effimero, just-in-time e just-enough privilege

ACTIVE DIRECTORY SECURITY / ITDR
Assicurati che AD sia pulito, compreso, configurato correttamente, monitorato attentamente e controllato rigorosamente

PASSWORD MANAGEMENT & SECURITY
Garantisci password complesse, univoche e non compromesse, con accessi semplificati e condivisione sicura

netwrix

Portfolio

DATA DISCOVERY & CLASSIFICATION

- Data Classification
- Enterprise Auditor

DATA ACCESS GOVERNANCE

- Auditor
- Enterprise Auditor
- 1Secure

DATA LOSS PREVENTION

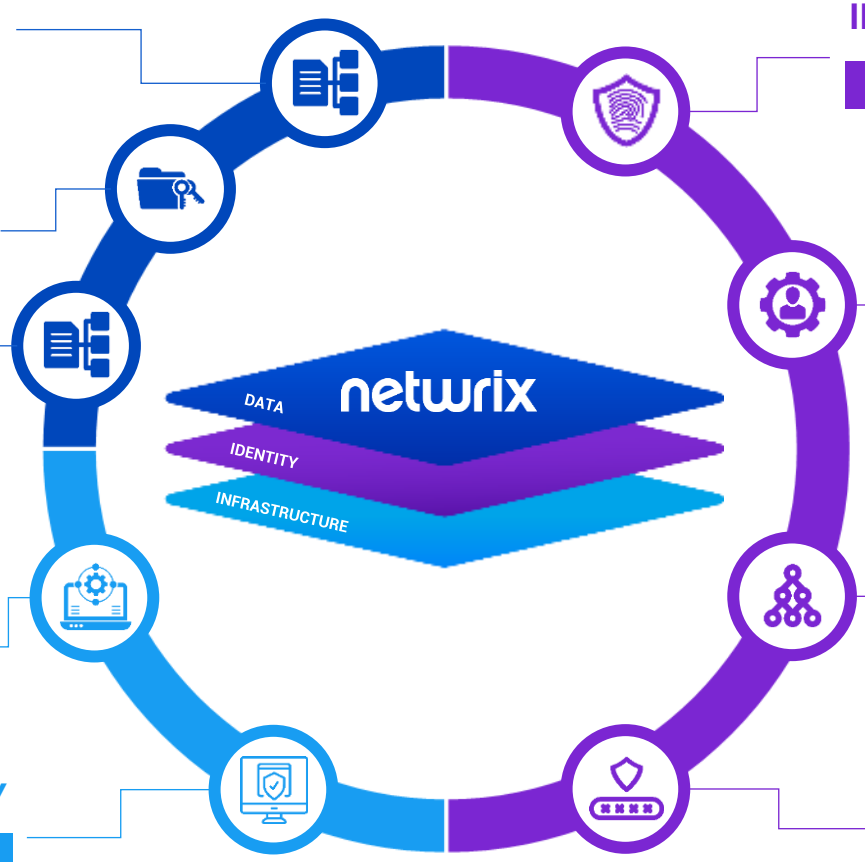
- Endpoint Protector

SECURITY CONFIGURATION MANAGEMENT

- Change Tracker
- Strongpoint

ENDPOINT MANAGEMENT & SECURITY

- Endpoint Protector
- PolicyPak



IDENTITY GOVERNANCE & ADMINISTRATION

- Usercube
- GroupID

PRIVILEGED ACCESS MANAGEMENT

- Privilege Secure
- PolicyPak

ACTIVE DIRECTORY SECURITY / ITDR

- Privilege Secure
- PolicyPak
- Recovery for AD
- Auditor
- Enterprise Auditor
- Threat Manager
- Threat Prevention
- GroupID
- PingCastle

PASSWORD MANAGEMENT & SECURITY

- Password Policy Enforcer
- Threat Prevention
- GroupID
- Password Secure

netwrix

Netwrix Product Portfolio

Netwrix Auditor	IT Auditing & Compliance Reporting
Netwrix Change Tracker	Security Configuration Management
Netwrix Data Classification	Data Discovery & Classification
Netwrix Password Policy Enforcer	Active Directory Password Policy Enforcement
Netwrix Password Secure	Password Lifecycle Management
Netwrix PolicyPak	Desktop Least Privilege and Policy Control
Netwrix Privilege Secure	Privileged Access Management
Netwrix 1Secure	SaaS-based IT Auditing & Compliance Reporting
new **Netwrix PingCastle**	Active Directory and Entra ID Security Assessment

Netwrix Enterprise Auditor	Data Access Governance
Netwrix Threat Manager	Threat Detection & Response
Netwrix Threat Prevention	Active Directory Security Policy Enforcement
Netwrix Recovery for Active Directory	Active Directory Rollback & Recovery
Netwrix Strongpoint	Salesforce and NetSuite Security & Compliance
Netwrix Usercube	Identity Governance & Administration
Netwrix GroupID	User and Group Management
Netwrix Endpoint Protector	Endpoint Data Loss Prevention

netwrix

Netwrix ti aiuta a rispettare le norme

Government

- **FedRAMP** — Federal Risk & Authorization Management Program
- **FISMA** — Federal Information Security Management Act
- **CMMC** — Cybersecurity Maturity Model Certification
- **CJIS** — Criminal Justice Information Services

Critical Infrastructure

- **NERC CIP** — North American Electric Reliability Corporation Critical Infrastructure Protection
- **NIS2** — Directive on Security of Network and Information Systems
- **CESC2M2** — Electricity Subsector Cybersecurity Capability Maturity Model

Finance

- **GLBA** — Financial Services Gramm-Leach-Bliley Act
- **PCI DSS** — Payment Card Industry Data Security Standard
- **SOX** — Sarbanes–Oxley Act
- **FINRA** — Financial Industry Regulatory Authority Guidelines

Education

- **FERPA** — Family Educational Rights and Privacy Act

Privacy

- **GDPR** — General Data Protection Regulation
- **CCPA** — California Consumer Privacy Act

Healthcare

- **HIPAA** — Health Insurance Portability and Accountability Act
- **HITRUST** — Health Information Trust Alliance

Frameworks

- **CIS CSC** — CIS Critical Security Controls
- **NIST CSF** — NIST Cybersecurity Framework

Telco

- **ISO 27011** — Information Security Management System

NIST Special Publications

- **NIST 800-53** — Security and Privacy Controls for Information Systems and Organizations
- **NIST 800-171** — Controlled Unclassified Information in Nonfederal Systems and Organizations

General

- **ISO 27001, 27002, 27015, and 27018** — Information Security Management System
- **COBIT** — Control Objectives for Information Technologies
- **SOC2** — Service Organization Control
- **NCCoE** — National Cybersecurity Center of Excellence
- **CISA** — Cybersecurity Information Sharing Act

netwrix

NIS 2

	Auditor	Data Classification	Endpoint Protector	Privilege Secure	Privilege Secure for Endpoints	Change Tracker	Password Secure	PingCastle	Recovery for Active Directory	GroupID	Usercube	Threat Manager	Threat Prevention
a) politiche di analisi dei rischi e di sicurezza dei sistemi informatici	✓	✓	✓			✓		✓		✓			
b) gestione degli incidenti	✓	✓	✓					✓				✓	✓
c) continuità operativa, come la gestione del backup e il ripristino in caso di disastro, e gestione delle crisi;	✓	✓			✓	✓			✓	✓	✓		
d) sicurezza della catena di approvvigionamento, compresi aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;	✓			✓	✓		✓	✓		✓	✓		
e) sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità;						✓							
f) strategie e procedure per valutare l'efficacia delle misure di gestione dei rischi di cybersicurezza;	✓		✓	✓	✓	✓	✓	✓		✓	✓		
g) pratiche di igiene informatica di base e formazione in materia di cybersicurezza;	✓		✓	✓	✓		✓						
h) politiche e procedure relative all'uso della crittografia e, se del caso, della cifratura			✓										
i) sicurezza delle risorse umane, strategie di controllo dell'accesso e gestione degli asset;				✓			✓			✓	✓		
j) uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, se del caso.				✓	✓		✓				✓		

NIST Cybersecurity Framework 2.0

Complete Functionality Mapping
https://www.netwrix.com/nist_cfs_controls_and_netwrix_functionality_mapping.html

		Auditor	Data Classification	Change Tracker	Privilege Secure	Enterprise Auditor
Identify (ID)	Asset Management	✓	✓			✓
	Risk Assessment	✓		✓		✓
	Improvement					
Protect (PR)	Identity Management, Authentication, and Access Control	✓	✓		✓	✓
	Awareness and Training					
	Data Security		✓			✓
	Platform Security			✓		
	Technology Infrastructure Resilience			✓		
Detect (DE)	Continuous Monitoring	✓	✓	✓	✓	✓
	Adverse Event Analysis				✓	✓
Respond (RS)	Incident Management	✓		✓	✓	✓
	Incident Analysis	✓		✓		✓
	Incident Response Reporting and Communication					
	Incident Mitigation	✓			✓	✓
Recover (RC)	Incident Recovery Plan Execution	✓	✓	✓		✓
	Incident Recovery Communication					

netwrix

ISO 27002

(Applicable to ISO 27001, 27011, 27015, and 27018)

Complete Functionality Mapping
https://www.netwrix.com/ISO_IEC_Compliance.html

	Auditor	Data Classification	Enterprise Auditor	Privilege Secure	Privilege Secure for Endpoints	Change Tracker	Password Secure
User endpoint devices					✓		
Privileged access rights	✓		✓	✓			
Information access restriction	✓	✓	✓	✓	✓		✓
Access to source code	✓		✓	✓			✓
Secure authentication	✓	✓	✓	✓	✓		✓
Capacity management						✓	
Protection against malware	✓		✓			✓	
Management of technical value	✓		✓			✓	
Configuration management	✓		✓			✓	
Information deletion	✓	✓	✓	✓	✓		
Data masking		✓					
Data leakage prevention		✓					
Information backup		✓					
Redundancy of information processing facilities		✓				✓	
Logging	✓	✓	✓	✓	✓	✓	✓
Monitoring activities	✓		✓	✓	✓		
Clock synchronization	✓	✓	✓	✓	✓	✓	✓
Use of Privileged utility programs	✓		✓	✓			
Installation of software on operational systems					✓	✓	
Network security							
Security of network services							
Segregation of networks							
Web filtering					✓		
Use of cryptography							✓
Secure Development lifecycle						✓	
Application Security requirements					✓	✓	
Secure system architecture and engineering principles						✓	
Secure coding							
Security testing in development and acceptance							
Outsourced development	✓		✓	✓			
Separation of development, test and production environments							
Change management						✓	
Test information							
Protection of information systems during audit	✓	✓	✓	✓	✓	✓	✓

CIS CSC

Complete Functionality Mapping
https://www.netwrix.com/cis_critical_security_controls_and_netwrix_functionality_mapping.html

	Auditor	Data Classification	Enterprise Auditor	Privilege Secure	Privilege Secure for Endpoints	Change Tracker	Password Secure	Recovery for Active Directory	GroupID	Usercube
Inventory and Control of Hardware Assets										
Inventory and Control of Software Assets	✓	✓	✓		✓	✓	✓	✓	✓	✓
Continuous Vulnerability Management	✓		✓	✓		✓		✓	✓	✓
Controlled Use of Administrative Privileges	✓		✓	✓					✓	✓
Secure Configuration for Hardware and Software						✓				
Maintenance, Monitoring, and Analysis of Audit Logs	✓		✓	✓		✓		✓	✓	✓
Email and Web Browser Protections					✓					
Malware Defense					✓	✓		✓		
Limitation and Control of Network Ports, Protocols, and Services				✓						
Data Recovery Capability								✓		
Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches						✓				
Boundary Defense	✓		✓	✓	✓					
Data Protection	✓	✓	✓					✓		
Controlled Access Based on a Need To Know	✓	✓	✓	✓	✓				✓	✓
Wireless Access Control	✓		✓	✓	✓		✓		✓	✓
Account Monitoring and Control	✓		✓	✓					✓	✓
Implement a Security Awareness and Training Program										
Application Software Security						✓				
Incident Response and Management	✓		✓	✓	✓	✓		✓	✓	✓
Penetration Tests and Red Team Exercises										

PCI DSS 4.0

Complete Functionality Mapping
https://www.netwrix.com/PCI_Compliance.html

	Auditor	Data Classification	Enterprise Auditor	Privilege Secure	Privilege Secure for Endpoints	Change Tracker	Password Secure	Recovery for Active Directory	GroupID	Usercube
Install and maintain a firewall configuration to protect cardholder data						✓				
Do not use vendor-supplied defaults for system passwords and other security parameters				✓			✓			✓
Protect stored cardholder data	✓	✓	✓		✓	✓				
Encrypt transmission of cardholder data across open, public networks		✓								
Protect all systems against malware and regularly update antivirus software or programs					✓	✓				
Develop and maintain secure systems and applications			✓	✓	✓	✓	✓	✓	✓	✓
Restrict access to cardholder data by business need to know	✓		✓	✓	✓				✓	✓
Identify and authenticate access to system components	✓			✓	✓				✓	✓
Restrict physical access to cardholder data										
Track and monitor all access to network resources and cardholder data	✓		✓	✓	✓	✓	✓			✓
Regularly test security systems and processes						✓				
Maintain a policy that addresses information security for all personnel	✓		✓		✓					✓

netwrix

Passaggi successivi

Richiedi la tuo Demo personalizzata

netwrix.it/demo

Scarica il white paper

"Autovalutazione della sicurezza AD"

netwrix.it/whitepaper

Scarica la soluzione

netwrix.it/pingcastle

Domande?

netwrix

Grazie!

cips

Per avere maggiori informazioni visita netwrix.it