Clusit Associazione Italiana per la Sicurezza Informatica

SECURITY SUMMIT

ASTREA Advanced Security, Training Research, Events Agency

Security Summit

Milano 19-20-21 marzo 2024

netwrix

cips

Sicurezza dei Dati, Identità e Infrastrutture:

L'Intreccio tra Risk Management, GDPR e Direttiva NIS2 e la sfida alle minacce informatiche

Maurizio Taglioretti – Regional Manager SEEUR – Netwrix

Veronica Conti – Sales Engineer – CIPS Informatica

Fabio Pelargonio – PS Engineer – Netwrix

19 marzo 2024 SALA ASIA C | 15:00 - 15:40


Vidnoz

Relatori

Maurizio Taglioretti

Regional Manager SEEUR, Netwrix

Appassionato di audit, compliance e sicurezza IT.

Socio di:

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 20 anni di esperienza. CNE, ITIL v4 ,Prince2 Practitioner

Socio di:

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

GDPR e Gestione del Rischio

Il GDPR richiede di considerare e gestire il **rischio** in diversi contesti normativi, tra cui i seguenti:

- Articolo 24: evidenzia la responsabilità del titolare del trattamento, che deve adottare misure adeguate per **identificare, valutare e gestire i rischi.**
- Articolo 25: obbliga il titolare del trattamento a proteggere i dati sin dalla fase di progettazione, tenendo conto delle **diverse possibilità e intensità dei rischi.**
- Articolo 32: impone al titolare e al responsabile del trattamento di assicurare un **livello di sicurezza adeguato al rischio**.
- Articolo 35: prevede l'obbligo di valutare l'impatto, seguendo una procedura formale, **quando si rileva un rischio elevato** persistente nel trattamento dei dati.
- Considerando 75 e 76: indicazioni sui i diritti e le libertà delle persone fisiche.

L’importanza del Risk Assessment

- Un aspetto rilevante della NIS2 è l’introduzione di un obbligo di risk assessment per le imprese coinvolte, che devono valutare e gestire i rischi cyber derivanti da fonti interne ed esterne. Questo implica anche di considerare le misure adottate dai propri fornitori e di monitorare la propria catena di fornitura, effettuando controlli regolari e accurati sulle terze parti coinvolte.

- In base ai risultati della valutazione dei rischi, la Direttiva NIS2 stabilisce una serie di misure tecniche e organizzative che le società classificate come “essenziali” e “importanti” devono rispettare.

NIS 2 in breve

① **Aumentare il livello della cyber-resilienza delle imprese nell'UE**

② **Ridurre le incoerenze tra le normative degli Stati membri**

③ **Migliorare la consapevolezza, la preparazione e le capacità di risposta**

> 50

> 10 M

18 Settori

Soggetti essenziali e importanti

Art. 3

sono considerati soggetti essenziali i seguenti:

a) soggetti di cui all'allegato I che superano i massimali per le medie imprese di cui all'articolo 2, paragrafo 1, dell'allegato della raccomandazione 2003/361/CE;

b) prestatori di servizi fiduciari qualificati e registri dei nomi di dominio di primo livello, nonché prestatori di servizi DNS, indipendentemente dalle loro dimensioni;

c) fornitori di reti pubbliche di comunicazione elettronica o di servizi di comunicazione elettronica accessibili al pubblico che si considerano medie imprese ai sensi dell'articolo 2, dell'allegato alla raccomandazione 2003/361/CE;

d) i soggetti della pubblica amministrazione di cui all'articolo 2, paragrafo 2, lettera f), punto i);

e) qualsiasi altro soggetto di cui all'allegato I o II che uno Stato membro identifica come soggetti essenziali ai sensi dell'articolo 2, paragrafo 2, lettere da b) a e);

sensi della direttiva (UE) 2022/2557, di cui all'articolo 2, paragrafo 3 della presente direttiva; g) se lo Stato membro lo prevede, i soggetti che tale Stato membro ha identificato prima del 16 gennaio 2023 come operatori di servizi essenziali a norma della direttiva (UE) 2016/1148 o del diritto

2. Ai fini della presente direttiva, sono considerati soggetti importanti i soggetti di una tipologia elencata negli allegati I o II che non sono considerati soggetti essenziali ai sensi del paragrafo 1 del presente articolo. Ciò comprende soggetti identificati dagli Stati membri come soggetti importanti ai sensi dell'articolo 2, paragrafo 2, lettere da b) a e); 3

I settori interessati

- Energia
- Trasporti
- Settore Bancario
- Infrastrutture dei mercati finanziari
- Settore Sanitario
- Acqua Potabile
- Acque Reflue
- Infrastrutture Digitali
- Gestione dei servizi TIC (business-to-business)
- Pubblica Amministrazione
- Spazio
- Servizi postali e di Corriere
- Gestione dei Rifiuti
- Fabbricazione, produzione e distribuzione di sostanze chimiche
- Produzione, trasformazione e distribuzione di alimenti
- Fabbricazione
- Fornitori di Servizi Digitali
- Ricerca

Le aziende interessate

La NIS 2 ha l'obiettivo di chiarire e uniformare la classificazione dei vari attori che rientrano nella sua sfera di applicazione, superando le ambiguità e le differenze della precedente Direttiva NIS. Il criterio adottato per distinguere tra entità essenziali e entità importanti è quello della dimensione del soggetto. La NIS 2, infatti, si applicherà a tutti quei soggetti pubblici o privati appartenenti alle categorie "alta criticità" o "altri settori critici" che:

> 50

1. **offrono i loro servizi o esercitano le loro attività all'interno dell'Unione**;

> 10 M

2. **sono qualificati come medie imprese secondo l'articolo 2, paragrafo 1, dell'allegato alla raccomandazione 2003/361/CE, o che superino i limiti per le medie imprese di cui al paragrafo 1 dello stesso articolo**.

(Articolo 2 Effettivi e soglie finanziarie che definiscono le categorie di imprese §1. La categoria delle microimprese, delle piccole imprese e delle medie imprese (PMI) è costituita da imprese che occupano meno di 250 persone, il cui fatturato annuo non supera i 50 milioni di euro oppure il cui totale di bilancio annuo non supera i 43 milioni di euro.)

I Fornitori di servizi (MSP)

(86) Tra i fornitori di servizi, i fornitori di servizi di sicurezza gestiti in settori quali la risposta agli incidenti, i test di penetrazione, gli audit di sicurezza e la consulenza svolgono un ruolo particolarmente importante nell'assistere i soggetti nei loro sforzi per la prevenzione e il rilevamento degli incidenti, la risposta agli stessi o la ripresa da essi. I fornitori di servizi di sicurezza gestiti sono stati tuttavia essi stessi bersaglio di attacchi informatici e, a causa della loro stretta integrazione nelle attività dei soggetti, presentano un particolare rischio. **I soggetti essenziali e importanti dovrebbero pertanto esercitare una maggiore diligenza nella selezione di un fornitore di servizi di sicurezza gestiti**

9. Gestione dei servizi TIC (business-to-business) — Fornitori di servizi gestiti — Fornitori di servizi di sicurezza gestiti

Quali misure adottare

Articolo 21 § 1
Misure di gestione dei rischi di cybersicurezza

1. Gli Stati membri provvedono affinché i soggetti essenziali e importanti adottino **misure tecniche, operative e organizzative adeguate e proporzionate** per **gestire i rischi posti alla sicurezza dei sistemi informatici e di rete** che tali soggetti utilizzano nelle loro attività **o nella fornitura dei loro servizi**, nonché per prevenire o ridurre al minimo l'impatto degli incidenti per i destinatari dei loro servizi e per altri servizi.

Tenuto conto delle conoscenze più aggiornate in materia e, se del caso, delle pertinenti norme europee e internazionali, nonché dei costi di attuazione, le misure di cui al primo comma assicurano un livello di sicurezza dei sistemi informatici e di rete **adeguato ai rischi esistenti**. Nel valutare la proporzionalità di tali misure, si tiene debitamente conto del grado di esposizione del soggetto a rischi, delle dimensioni del soggetto e della probabilità che si verifichino incidenti, nonché della loro gravità, compreso il loro impatto sociale ed economico.

Quali misure adottare

Art.21 § 2.

Le misure di cui al paragrafo 1 sono basate su un approccio multirischio mirante a proteggere i sistemi informatici e di rete e il loro ambiente fisico da incidenti e comprendono almeno gli elementi seguenti:

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.

Obblighi di segnalazione

Ciascuno Stato membro provvede affinché i soggetti essenziali e importanti notifichino senza indebito ritardo al proprio CSIRT o, se opportuno, alla propria autorità competente, eventuali incidenti che hanno un impatto significativo

- senza indebito ritardo, e comunque entro 24 ore da quando sono venuti a conoscenza dell'incidente significativo, un preallarme che, se opportuno, indichi se l'incidente significativo è sospettato di essere il risultato di atti illegittimi o malevoli o può avere un impatto transfrontaliero;
- senza indebito ritardo, e comunque entro 72 ore da quando sono venuti a conoscenza dell'incidente significativo, una notifica dell'incidente che, se opportuno, aggiorni le informazioni di cui alla lettera a) e indichi una valutazione iniziale dell'incidente significativo, comprensiva della sua gravità e del suo impatto, nonché, ove disponibili, gli indicatori di compromissione

Gli Stati membri provvedono affinché, ai fini della notifica a norma del paragrafo 1, i soggetti interessati trasmettano al CSIRT o, se opportuno, all'autorità competente:

d) una relazione finale entro un mese dalla trasmissione della notifica dell'incidente di cui alla lettera b), che comprenda:

i) una descrizione dettagliata dell'incidente, comprensiva della sua gravità e del suo impatto;

ii) il tipo di minaccia o la causa di fondo che ha probabilmente innescato l'incidente;

iii) le misure di attenuazione adottate e in corso;

iv) se opportuno, l'impatto transfrontaliero dell'incidente;

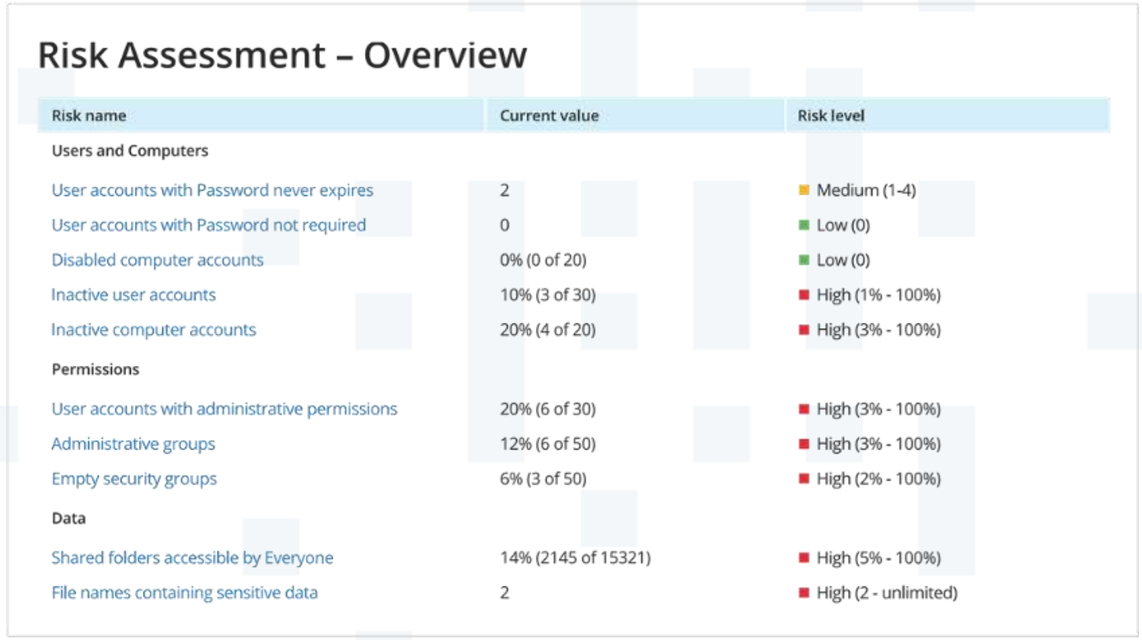
L’Art. §21.2.a richiede di implementare politiche di analisi dei rischi e di sicurezza dei sistemi informatici, quali Soluzioni Netwrix possono aiutare un’azienda in questo processo?

Politiche di analisi dei rischi e di sicurezza dei sistemi informatici

Risk Assessment

Netwrix Auditor permette di valutare i rischi di sicurezza di dati, identità e infrastruttura come richiesto dall'**Art. §21.2.a: Politiche di analisi dei rischi e di sicurezza dei sistemi informatici**

Vengono identificate le lacune di sicurezza di dati, identità e infrastruttura, quali un numero elevato di autorizzazioni assegnate in maniera diretta o troppi account utente inattivi. Questi parametri di sicurezza vengono valutati continuamente e visualizzati attraverso una dashboard intuitiva, semplice e interattiva che permette di intervenire in tempo reale sui rischi.

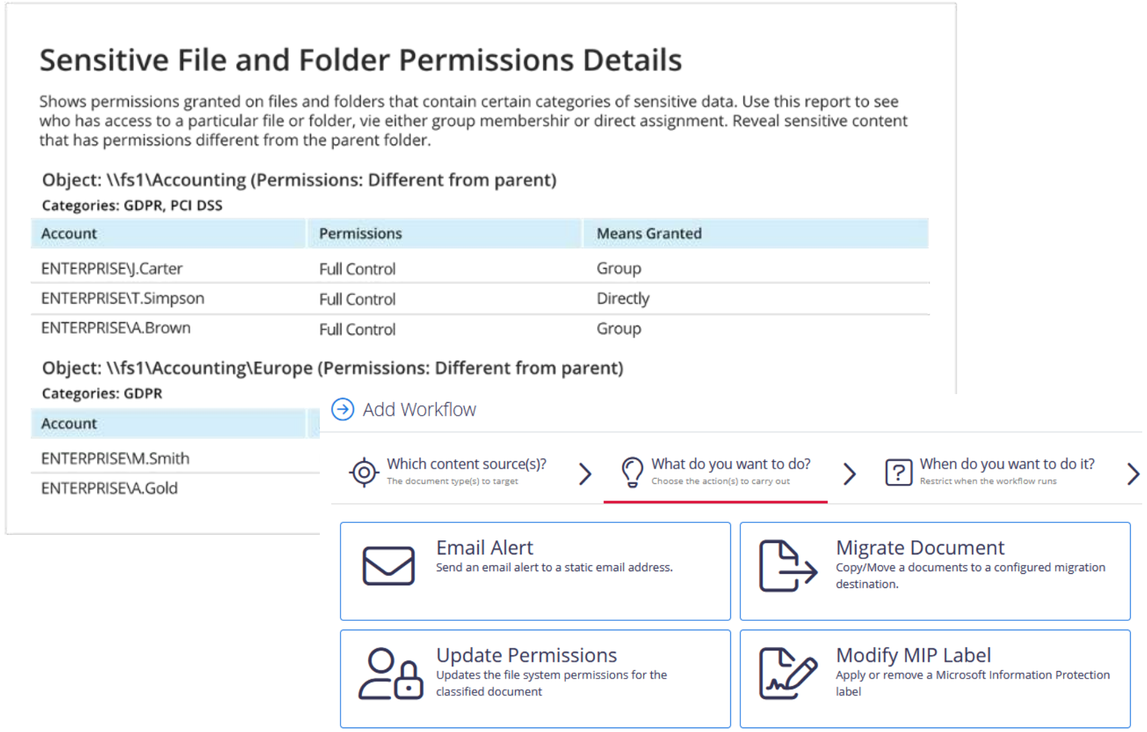


Risk Assessment – Overview

Risk name	Current value	Risk level
Users and Computers		
User accounts with Password never expires	2	Medium (1-4)
User accounts with Password not required	0	Low (0)
Disabled computer accounts	0% (0 of 20)	Low (0)
Inactive user accounts	10% (3 of 30)	High (1% - 100%)
Inactive computer accounts	20% (4 of 20)	High (3% - 100%)
Permissions		
User accounts with administrative permissions	20% (6 of 30)	High (3% - 100%)
Administrative groups	12% (6 of 50)	High (3% - 100%)
Empty security groups	6% (3 of 50)	High (2% - 100%)
Data		
Shared folders accessible by Everyone	14% (2145 of 15321)	High (5% - 100%)
File names containing sensitive data	2	High (2 - unlimited)

Netwrix Auditor

Politiche di analisi dei rischi e di sicurezza dei sistemi informatici



Vengono semplificate le regolari attestazioni di privilegio

Netwrix Auditor e Data Classification permettono di scoprire chi ha accesso a quali dati sensibili e in che modo ha ottenuto quell'accesso, abilitano i proprietari dei dati a verificare regolarmente che tali diritti siano in linea con le esigenze aziendali. In caso contrario, sarà più semplice capire quali autorizzazioni in eccesso rimuovere per applicare il **principio del minimo privilegio** e mantenere il rischio a un livello accettabile.

Possibilità di mettere automaticamente in quarantena i dati sensibili per ridurre il rischio di una violazione o di una perdita

Se un documento sensibile si trova in una posizione inaspettata, viene spostato automaticamente in un'area di quarantena fino a quando non verrà stabilito dove deve essere archiviato e chi deve accedervi.

Bloccare immediatamente i dati sensibili sovraesposti

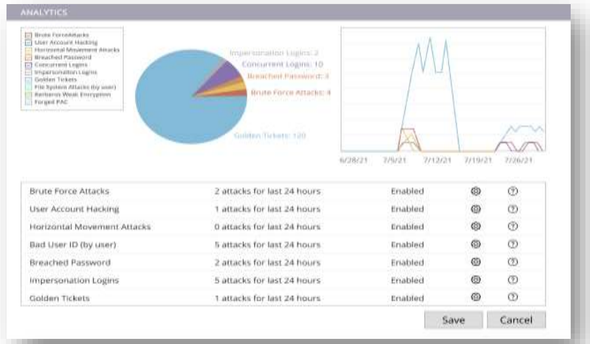
Se i controlli di accesso relativi ai dati sensibili non sono appropriati al rischio, rimuovi automaticamente tutti i diritti alla lettura o modifica di queste informazioni dai gruppi di accesso globali, quali Everyone.

Netwrix Auditor **Netwrix Data Classification**

Quali soluzioni Netwrix possiamo suggerire per adeguarsi all’ART. §21.2.b sulla gestione degli incidenti, nonché di ottemperare agli obblighi di segnalazione come previsto dall'ART. 23?

Gestione degli incidenti e obblighi di segnalazione

Netwrix StealthINTERCEPT



Netwrix StealthINTERCEPT **avvisa in tempo reale** in merito a modifiche, autenticazioni e altri **eventi sospetti o rischiosi** all'interno dell'infrastruttura in modo da darti la possibilità di impedire che si trasformino in violazioni.

Per Active Directory e File System, StealthINTERCEPT combina un flusso di attività di audit arricchito e ottimizzato con dati contestuali rilevanti per costruire efficacemente profili comportamentali dell'organizzazione utilizzando algoritmi di apprendimento automatico non supervisionati.

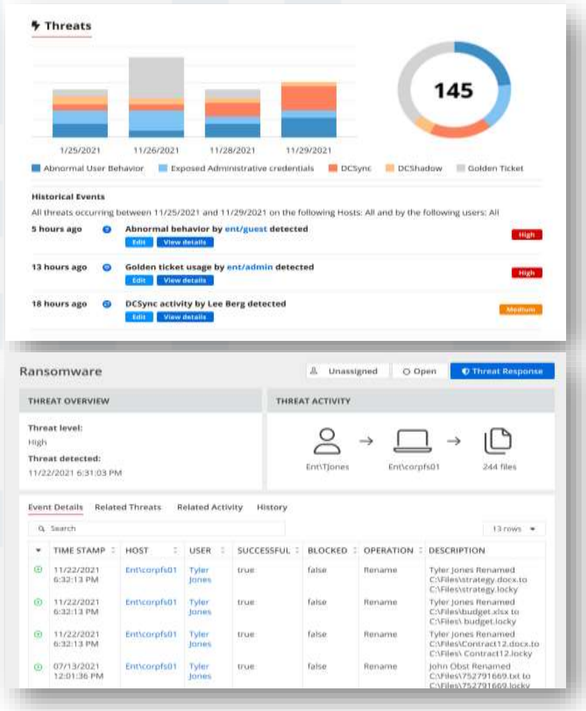
Inoltre, ti consente innanzitutto di impedire che si verifichino gli eventi critici.

Netwrix Threat Manager

Netwrix Threat Manager è una soluzione di **rilevamento e risposta alle minacce in tempo reale** creata appositamente per proteggere le credenziali e i dati di un'organizzazione.

Rispondi immediatamente al rilevamento delle minacce sfruttando l'esauriente catalogo di azioni di risposta preconfigurate o integrando Netwrix Threat Manager nei processi aziendali, utilizzando PowerShell o strutture webhook.

Il risultato è la capacità di rilevare, correlare e rispondere a comportamenti anomali e attacchi avanzati con una precisione e una velocità senza precedenti.



Netwrix StealthINTERCEPT

Netwrix Threat Manager

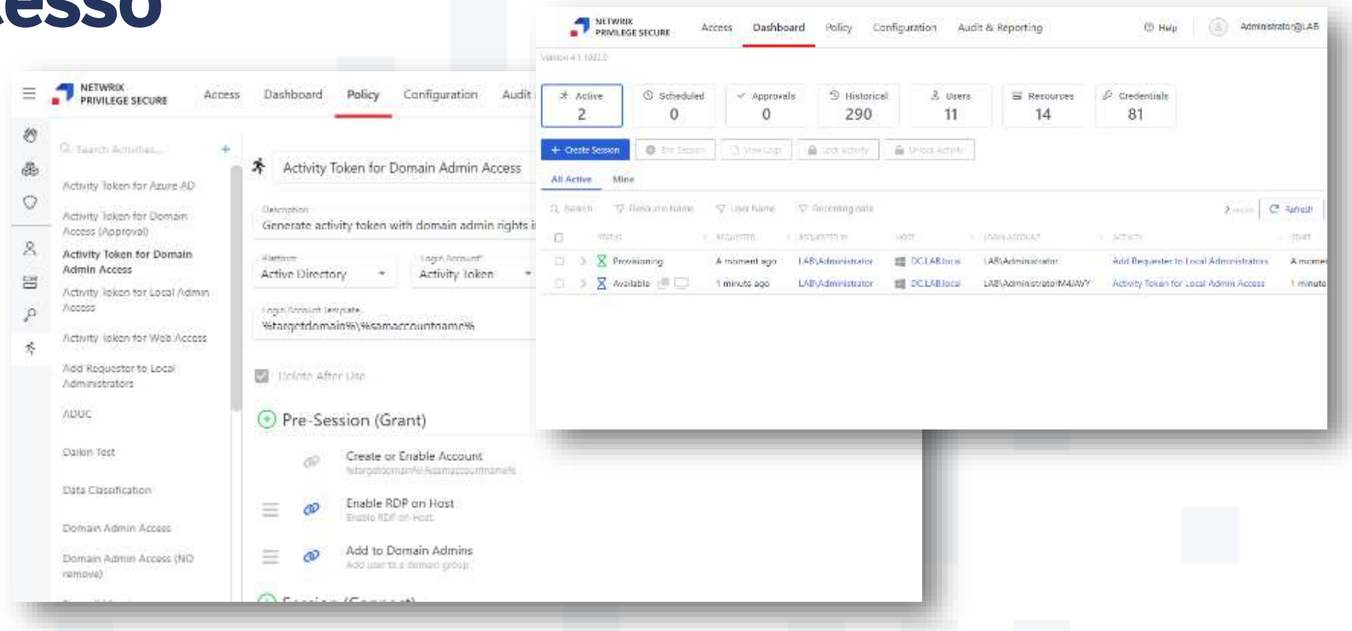
Altro punto importante è quello previsto dall’art. §21.2.d relativamente alla sicurezza della catena di approvvigionamento (supply chain) al quale possiamo affiancare anche l’ART. §21.2.i che richiede di implementare strategie di controllo dell'accesso e gestione degli asset; come possiamo rispondere?

Strategie di controllo dell'accesso

Privilege Access Management

Ridurre la superficie di attacco rimuovendo i privilegi permanenti

- Rimuovere i privilegi permanenti per ridurre i rischi
- Concedere l'accesso giusto agli utenti giusti
- Protezione dei diritti di amministratore locale
- Ridurre al minimo la superficie di attacco ripulendo gli oggetti con accesso privilegiato
- Proteggere gli account di servizio e quelli integrati
- Avanzare verso la **ZERO TRUST**



Just-in-Time Orchestration

Creare ciò che serve per svolgere un'attività specifica nel momento in cui serve, e rimuovere la superficie di attacco quando non la si utilizza.

Identity Orchestration

- Create / Remove Accounts
- Enable / Disable Accounts

Privilege Orchestration

- Add / Remove Permissions
- Enforce Group Membership

Endpoint Orchestration

- Enable/Disable RDP
- Purge Kerberos Tickets
- Pre/Post File Comparison
- Dynamic SMB Shares
- Custom PowerShell
- Dynamic sudoers

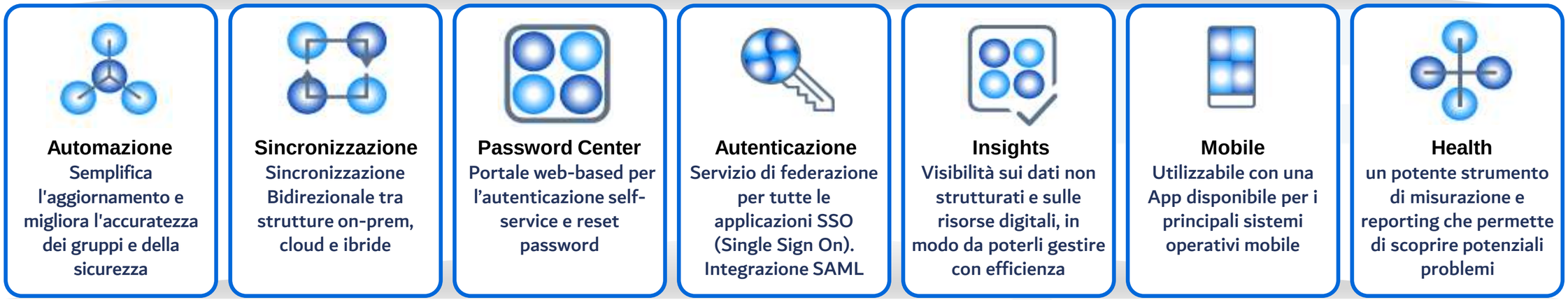
Netwrix Privilege Secure

Strategie di controllo dell'accesso

Gestione automatizzata dei gruppi per semplificare e proteggere Active Directory, Azure e Microsoft 365

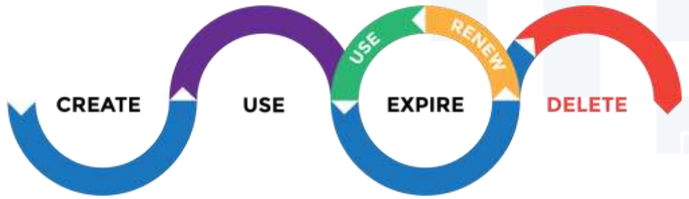
Semplifica la gestione di tutte le modifiche, le richieste e i requisiti che l'IT riceve ogni giorno.

Le liste di distribuzione, i gruppi di sicurezza e i gruppi di Office 365 sono sempre aggiornati, aumentando l'efficienza. Gli utenti sono in grado di eseguire le attività più comuni in modo indipendente, riducendo le chiamate all'help desk. I rischi per la sicurezza sono significativamente ridotti o eliminati del tutto.

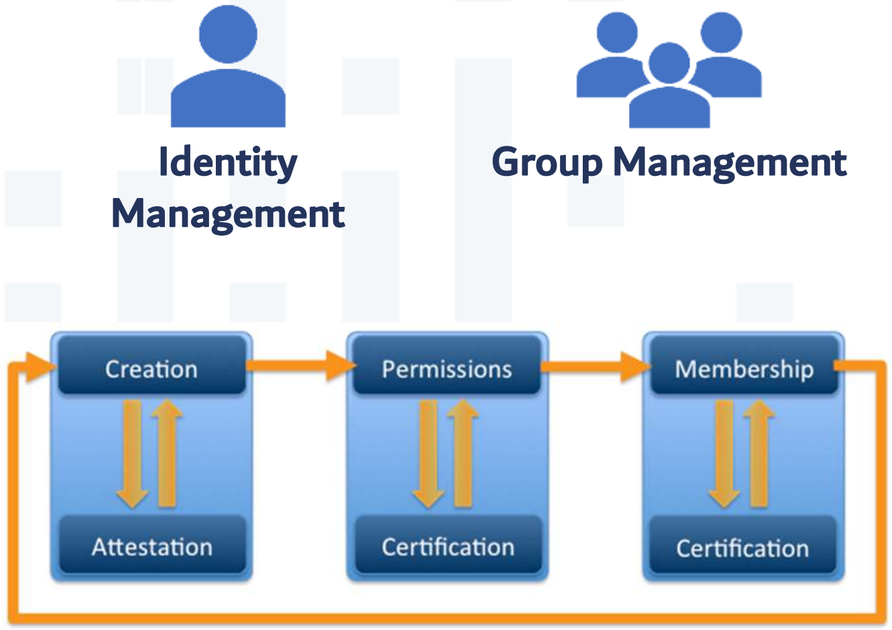


Netwrix GroupID

Strategie di controllo dell'accesso

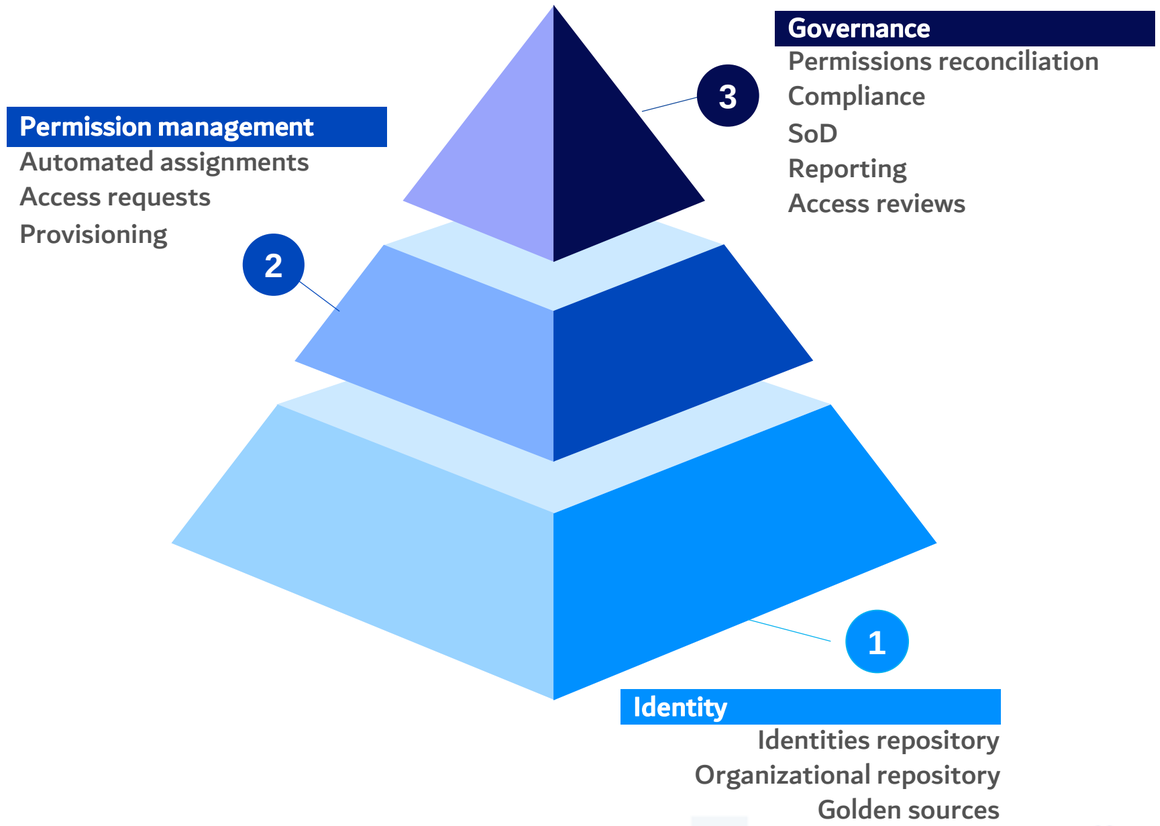


- Provisioning oggetti utente da una fonte autorevole
- Visualizzazione di utenti, gruppi, appartenenze e attributi
- Collegare gli oggetti tra gli identity stores
- Stabilire una chiara gerarchia manageriale, inclusa la gestione a linee tratteggiate
- Deprovisionare gli account utente al momento giusto
- Valutare le autorizzazioni delle risorse on-premise e cloud
- Trasferire e terminare gli account con la semplice pressione di un tasto
- Consentire ai manager di gestire i loro rapporti diretti, i gruppi e le autorizzazioni
- Sbloccare gli account e reimpostare le password



Netwrix GroupID

Strategie di controllo dell'accesso



Il giusto accesso alle cose giuste al momento giusto

- Usercube crea un repository di organizzazioni, siti, utenti e risorse, da diverse fonti, per diventare il luogo centralizzato per informazioni affidabili ed esaurienti.
- Ciascun utente può presentare una richiesta per ottenere, modificare o revocare diritti di accesso o apparecchiature per gli utenti nel proprio ambito. I flussi di lavoro consentono di inviare la richiesta alle persone appropriate per ottenere l'approvazione e/o iniziare a elaborare la richiesta il prima possibile.
- IGA riunisce tutti i processi della tua organizzazione per consentire a ogni individuo identificato di avere i diritti di accesso corretti al momento giusto per le giuste ragioni.

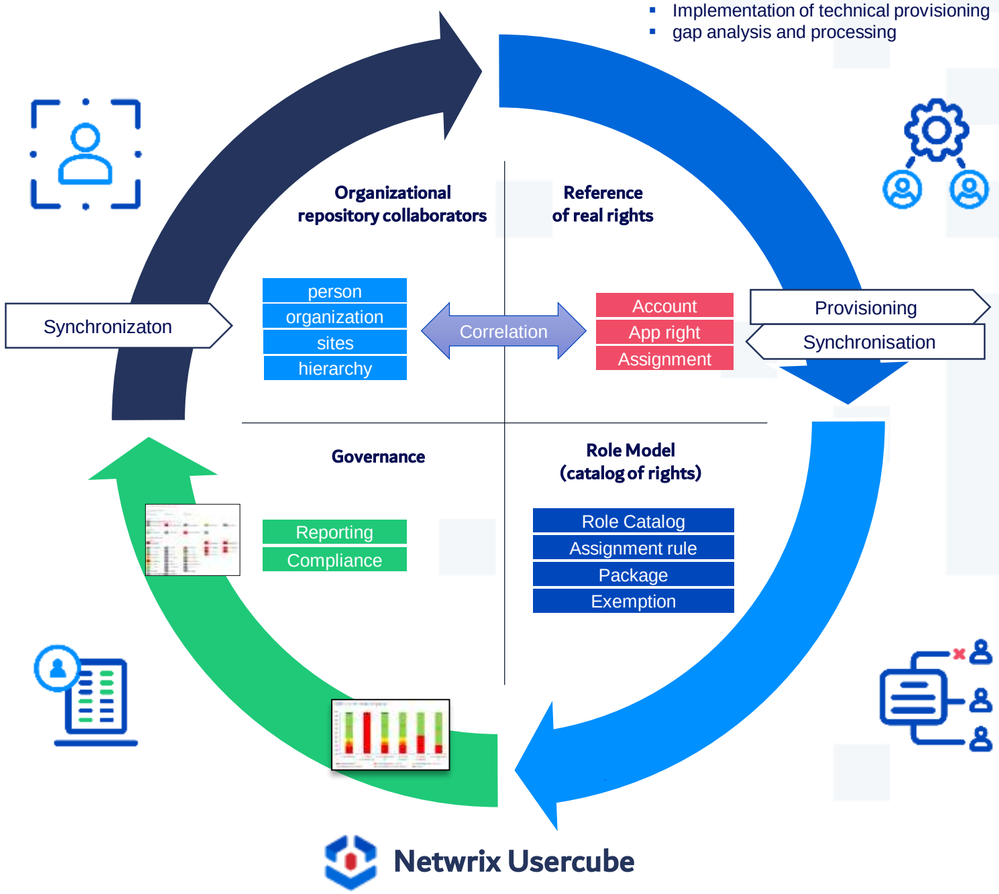
Netwrix Usercube

Strategie di controllo dell'accesso

Functional Architecture

Entry / Mobility / Exit Management

- J/M/L management
- Repository administration



Master data

- Implementation of technical provisioning
- gap analysis and processing

Provisioning, Synchronization and Reconciliation

Information System

IT technical resources

Account | Applications Profils | Groups AD / LDAP | Etc..

- AD, Exchange, Notes, O365, Gsuite…
- Appli. Métiers, CRM, ERP, GED, PLM…
- AS400, RACF, TSS
- Dotations, Badges, Bureaux…
- ITSM, ticketing

- Organize certification campaigns (compliance)
- Recertify (manager / app owner)
- Gap Review
- Analytics (BI)

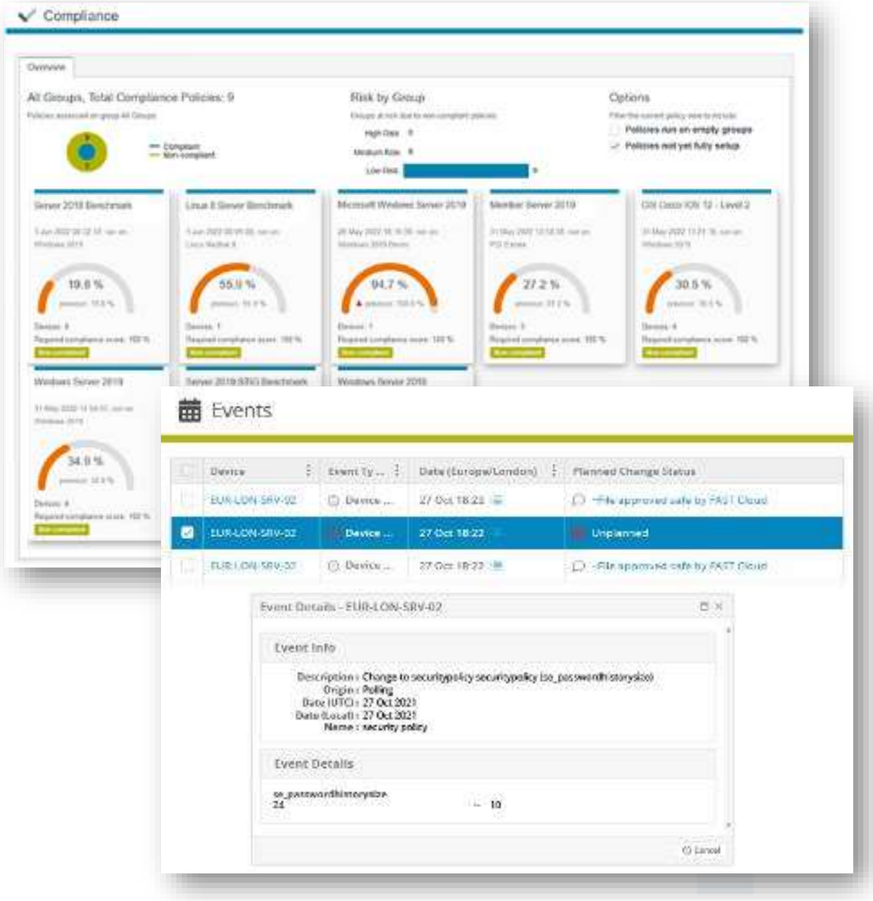
Governance

- Management of employee rights
- Approval of sensitive rights
- Role model administration
- Simulation
- Role Mining (AI)

identity rights management

Non meno importante quanto previsto dall’ART. §21.2.e in merito a sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informatici e di rete, compresa la gestione e la divulgazione delle vulnerabilità; quali soluzioni Netwrix propone?

Gestione delle vulnerabilità



System Hardening-File Integrity Monitoring-Compliance & Forensic Analysis

- Netwrix Change Tracker riduce il "rumore del cambiamento" e i falsi positivi di oltre il 90% creando un insieme di regole di modifica pianificate. Consente l'approvazione automatica dei file legittimi in base alla reputazione grazie al servizio Netwrix FAST Threat Intelligence. Verifica che i file di sistema più importanti siano autentici effettuando un controllo incrociato con un database di oltre 10 miliardi di reputazioni di file.
- Change Tracker ha una capacità di apprendimento automatico per estendere rapidamente le regole di modifica pianificate esistenti per acquisire eventi non pianificati rilevanti o persino per creare nuove regole di modifica pianificate intelligenti al volo.

Controlli CIS automatizzati - Compliance continua

- Riduci il lavoro necessario per dimostrare la conformità automatizzando le attività ripetitive e utilizzando **oltre 250 report** certificati CIS che comprendono NIST, PCI DSS, CMMC, STIG e NERC CIP.

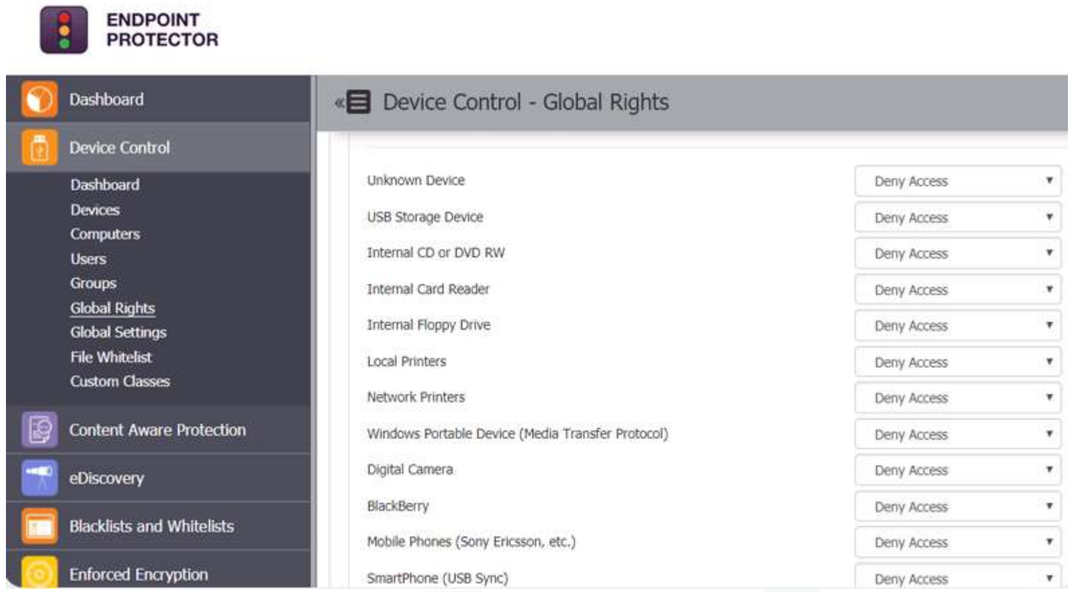
Netwrix Change Tracker Netwrix Threat Manager

Per quanto riportato dall'ART. §21.2 ai punti g.,h. e i. relativamente alle pratiche di igiene informatica di base e formazione, politiche di cifratura e sicurezza delle risorse umane e controllo degli accessi, quali soluzioni Netwrix propone orientate alla Data Loss Prevention?

Igiene di base, formazione, cifratura e controlli

Rilevazione, monitoraggio e protezione dei dati sensibili attraverso gli endpoint dei dipendenti

- Protezione dei dati: controllo dei flussi di spostamento dei dati in uso, creazione di criteri di gestione a scopo formativo e di protezione
- Minacce interne: previene le perdite di informazioni da parte di utenti malintenzionati, negligenti o compromessi
- Protezione continua: indipendente dalla posizione del dipendente, sia per team remoti che endpoint offline
- Estensione dei criteri di controllo dei dispositivi applicando la crittografia dei dati spostati su archivi rimovibili. Salvaguarda i dati in transito e garantisce la protezione dei dati sensibili in caso di smarrimento o furto del dispositivo USB
- Supporto multi piattaforma



Device Control

Content-Aware Protection

Enforced Encryption

eDiscovery

Q&A

Vieni a trovarci al nostro stand!

Contatti:
maurizio.taglioretti@netwrix.com
fabio.pelargonio@netwrix.com
veronica.conti@cips.it

www.netwrix.it

www.cips.it

Clusit Associazione Italiana per la Sicurezza Informatica

SECURITY SUMMIT