SECURITY SUMMIT

Security Summit

Milano 17-18-19 marzo 2026

Clusit

ASTREA

SALA ASIA B | 17 marzo 2026 | 14:20 - 15:00

L'AI non vi attacca, sta già usando i vostri dati! Dimenticate l'AI for Security perché la "Security FOR AI" è la vera priorità del 2026

Dominare Dati e Identità con DSPM e ISPM.

Maurizio Taglioretti | Director EMEA South & Benelux
Fabio Pelargonio | Senior Solutions Engineer

netwrix

Clusit

SECURITY SUMMIT

ASTREA

Clusit SECURITY SUMMIT ASTREA

netwrix

ACCELERATE

Clusit SECURITY SUMMIT ASTREA

netwrix

Benvenuti

Clusit SECURITY SUMMIT ASTREA

netwrix ACCELERATE

Maurizio Taglioretti
Director EMEA South & Benelux
Netwrix

Fabio Pelargonio
Senior Solutions Engineer
Netwrix

I rischi emergenti

CORRIERE DELLA SERA — L'Economia

TECNOLOGIA

Cos'è lo «shadow Ai» e perché preoccupa le aziende: i rischi cyber per i dipendenti «infedeli»

di Redazione Economia

Shadow Ai, 7 lavoratori su 10 usano l'intelligenza artificiale (anche non autorizzata): il rischio hacker e privacy

Cronaca Esteri Politica ...

Artificiale e guerre

L'esercito statunitense avrebbe utilizzato Anthropic Claude negli attacchi contro l'Iran

La rivelazione è del Washington Post. Trump il giorno prima dell'attacco si era scagliato contro Anthropic per il rifiuto dell'azienda di Intelligenza Artificiale di continuare a collaborare con il Pentagono per ragioni etiche

CORPORATE NEWS

Claude di Anthropic

di Serena Zagami (MF-Newswires)

02 marzo 2026, 16:22

Dario Amodei, ceo di Anthropic

La causa del blackout che ha portato a migliaia di segnalazioni da parte degli utenti non è chiara. La società fondata da Dario Amodei ha dichiarato che sono stati rilevati «errori significativi» in alcuni servizi e che sta indagando sul problema

CORRIERE TV

regolarmente strumenti di GenAI. Ma desta

Home › TechTarget › SearchSecurity › Cybersecurity

L'uso non autorizzato dell'intelligenza artificiale da parte dei dipendenti sta ridefinendo le politiche aziendali e mettendo alla prova la leadership IT. Ecco le mosse che i CIO devono

Principali preoccupazioni per le aziende e per i CIO

AD/Permessi, rischio e esposizione ai privilegi

Mancanza di visibilità/governance su AD + condivisioni file + cloud

Audit manuale/ Processi di compliance / Debole identity governance

Lacune nei sistemi Endpoint e DLP
Fuga di Proprietà Intellettuale/ Copertura dei diversi OS/ complessità

AI Readiness/ Governance e sicurezza dei dati per l'IA

"Nel 2025 abbiamo passato il tempo a chiederci come l'AI potesse aiutarci a scrivere codice più sicuro.

Nel 2026, la realtà ci ha presentato il conto:
l'AI non sta scrivendo malware, sta semplicemente leggendo i vostri dati non protetti perché glieli stiamo offrendo noi su un piatto d'argento. Oggi non parliamo di come usare l'AI, ma di come sopravvivere all'AI che avete già in casa."

I 3 "Blind Spot" della GenAI Governance

1. L'Eredità Tossica (The Permissions Debt)

- Il problema: L'AI non rispetta il "Least Privilege", rispetta ciò che può leggere. Se avete cartelle Sharepoint o database con permessi Everyone o gruppi Legacy sovradimensionati, l'AI li indicizzerà tutti.
- L'impatto: Un dipendente chiede all'AI "Qual è il budget per i licenziamenti?" e l'AI risponde attingendo a file che l'utente non sapeva nemmeno di poter vedere.
- **Perché è un blind spot**: Le aziende monitorano gli accessi diretti, ma non l'accessibilità potenziale dei modelli LLM.

2. L'Identità Sintetica e le API "Ghost«

- **Il problema:** Le identità non sono più solo umane. L'AI comunica tramite Service Principal, Bot e integrazioni API che spesso hanno privilegi amministrativi "per comodità".
- **L'impatto:** Un'app AI compromessa o mal configurata può esfiltrare dati su scala massiva agendo come un utente legittimo iper-privilegiato.
- **Perché è un blind spot:** L'**ISPM** tradizionale guarda l'utente umano, ma ignora le relazioni di trust tra il modello AI e l'infrastruttura dati.

3. La "Liquidità" del Dato Sensibile (The Prompt Leakage)

- **Il problema:** Il dato non esce più tramite un file allegato (bloccato dal vecchio DLP), ma tramite stringhe di testo (Prompt). Il dato diventa "liquido" e cambia forma.
- **L'impatto:** Inserire codice sorgente o dati PII in un prompt per "ottimizzarli" significa regalare quel dato alla base di addestramento del modello (Shadow AI).
- **Perché è un blind spot:** Il **DSPM** classico classifica i file, ma non capisce il *contesto* del flusso di dati verso i LLM esterni.

Blueprint Strategico – Architettura Unificata Dati-Identità

Fase 1: Discovery & Classification (DSPM Layer)

- **Azione:** Scansione automatizzata di tutti i repository (Cloud, On-Prem, SaaS).
- **Obiettivo:** Identificare dove risiedono i "Gioielli della Corona" (Dati PII, Proprietà Intellettuale, Segreti Industriali) che l'AI potrebbe ingerire.
- **Key Question:** "Cosa può vedere l'AI che non dovrebbe essere visto?"

Fase 2: Rightsizing & Hardening (ISPM Layer)

- **Azione:** Eliminazione del "Debito di Permessi". Rimozione degli Shadow Admin e chiusura degli accessi eccessivi.
- **Obiettivo:** Applicare il *Zero Trust* reale. Se l'utente non ha bisogno di un dato, l'AI che agisce per suo conto non deve poterlo leggere.
- **Key Question:** "Chi ha i privilegi per alimentare i modelli LLM?"

Blueprint Strategico – Architettura Unificata Dati-Identità

Fase 3: Continuous Governance (The Unified Bridge)

•**Azione:** Monitoraggio dei comportamenti anomali. Allerta immediata se un'identità (umana o bot) inizia a estrarre volumi insoliti di dati verso vettori AI.

•**Obiettivo:** Rilevare la *Shadow AI* in tempo reale.

•**Key Question:** *"Il comportamento dell'identità è coerente con la sensibilità del dato trattato?"*

Fase 4: Remediation & Enforcement

•**Azione:** Risposta automatizzata. Revoca dei privilegi o blocco del flusso di dati se viene rilevata una violazione della policy di "Security FOR AI".

•**Obiettivo:** Chiudere il cerchio della resilienza.

•**Key Question:** "*Siamo in grado di bloccare un leak di dati verso l'AI prima che il danno sia irreversibile?"*

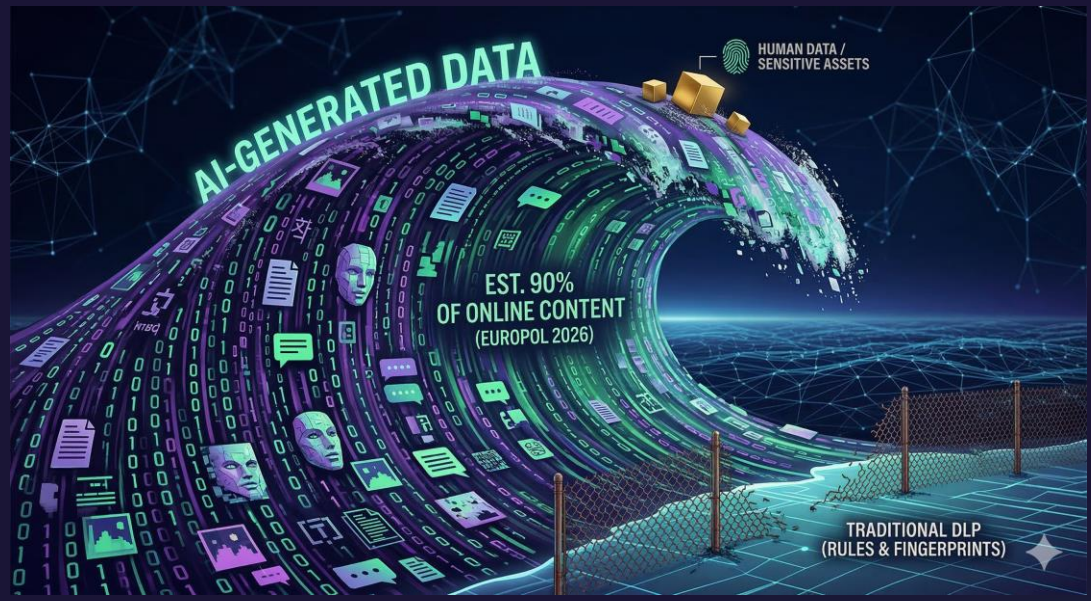
L'Anno del Sorpasso. Quando il Dato è 90% AI-Generated.

La Statistica Shock: "Entro la fine di quest'anno, il **90% dei contenuti digitali** sarà generato da algoritmi, non da esseri umani." (*Fonte: Europol Innovation Center*).

Il Paradosso del Controllo:
Stiamo cercando di proteggere una massa di dati infinita e "liquida" con strumenti nati per dati statici e strutturati.

Perché il DLP Tradizionale è KO:

- **Volume Esponenziale:** Le regole manuali e le "reg-ex" non possono scalare contro miliardi di nuovi file sintetici.
- **Mutazione del Dato:** L'AI rielabora il contenuto. Se un dato sensibile viene "riassunto" o "tradotto" da un LLM, il vecchio DLP non riconosce più l'impronta (fingerprint) originale.
- **La Cecità del Contesto:** Il DLP classico vede *cosa* esce, ma non capisce *perché* e *verso quale* modello AI si sta muovendo.

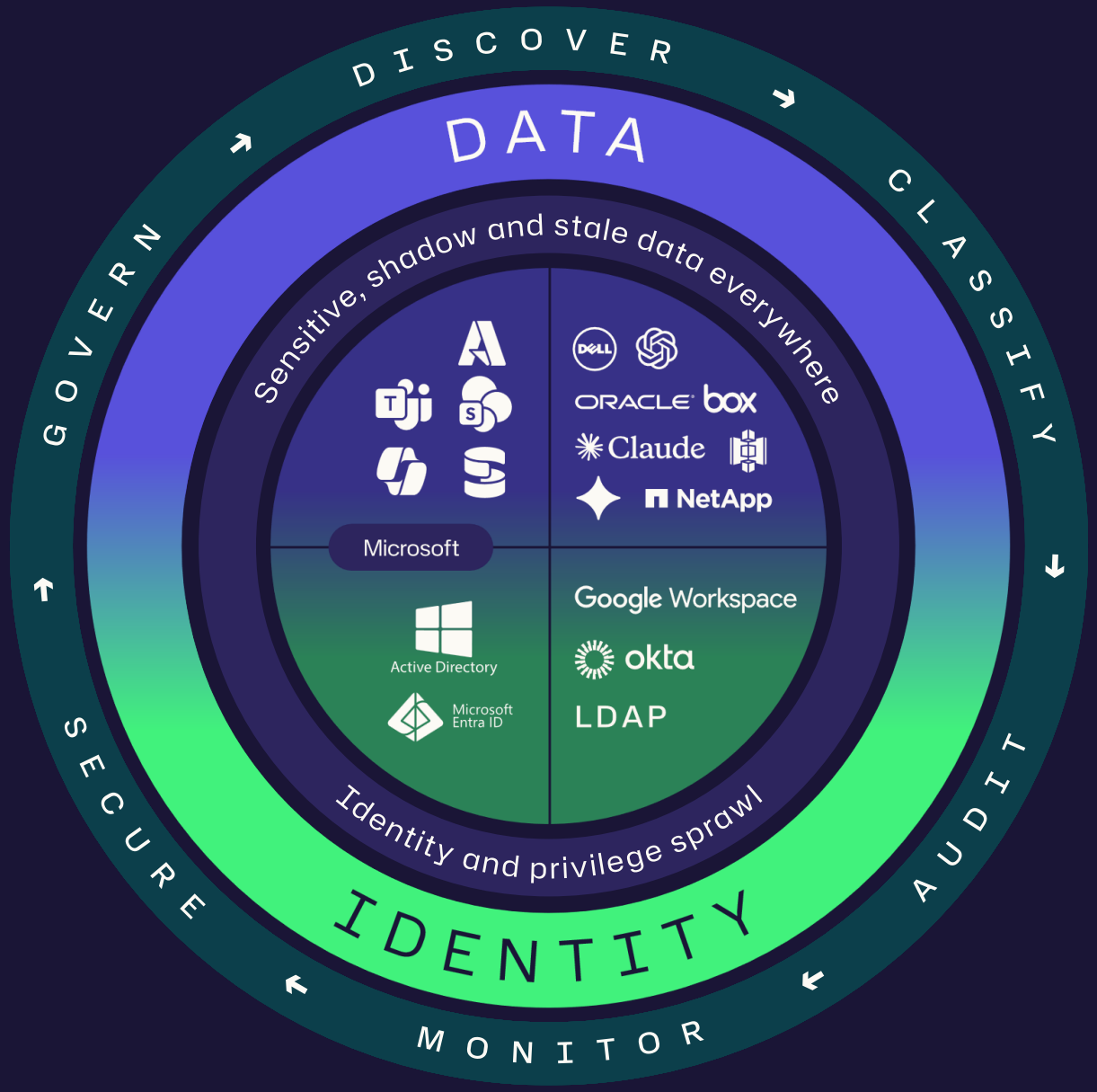


Il Punto di Rottura

*"Senza **DSPM** (per capire il valore del dato) e **ISPM** (per capire l'autorità dell'identità), stiamo cercando di svuotare l'oceano con un cucchiaino."*

In un mondo guidato dall'intelligenza artificiale, l'identità è l'obiettivo e i dati sono il premio.

Cosa facciamo in Netwrix



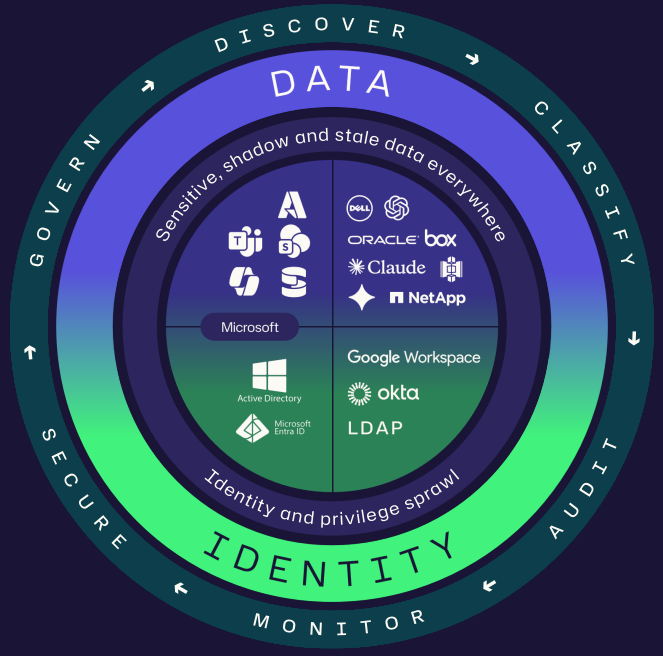
Cosa facciamo in Netwrix

Data Security Posture Management
Scansiona i dati e risolvi problemi di sicurezza

Data Access Governance
Riduci il rischio di violazione dei dati con il minimo privilegio

Data Loss Prevention
Previeni la perdita di dati sensibili su ogni endpoint

Data Discovery & Classification
Rileva e classifica i dati sensibili automaticamente



AI Governance
Proteggei i dati sensibili utilizzati da strumenti Copilot e LLM

Directory Security
Monitora i sistemi di identità e ripristina dopo gli attacchi

Identity Security Posture Management
Identificazione, priorità e risoluzione delle vulnerabilità delle identità

Identity Threat Detection & Response
Prevenire, rilevare e rispondere agli attacchi di identità

Identity Governance & Administration
Gestione completa del ciclo di vita delle identità

Privileged Access Management
Elimina i privilegi permanenti per ridurre i rischi di accesso

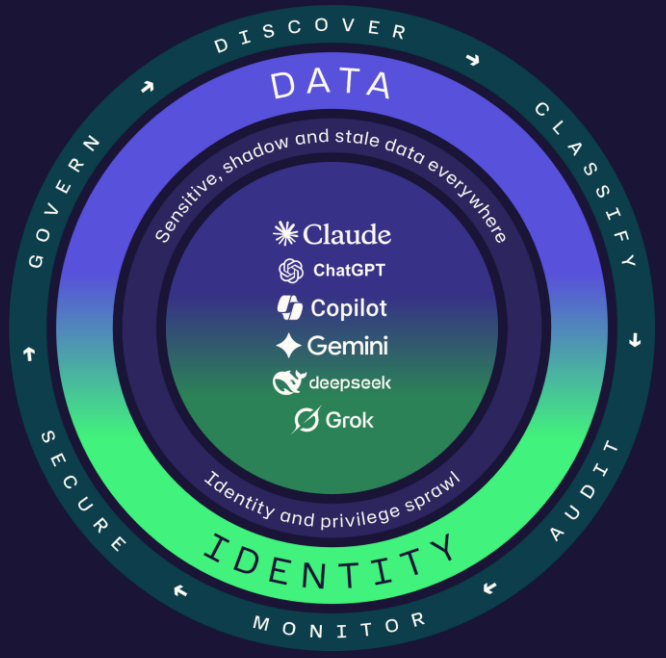
Netwrix: Basi della sicurezza per l'intelligenza artificiale aziendale

Data Security Posture Management
Sapere quali sono i dati esposti alla tua AI

Data Access Governance
Capire a quali dati ogni modello può accedere

Data Loss Prevention
Prevenire la perdita di dati sensibili causa dei motori di AI

Data Discovery & Classification
Classifica tutti i dati acceduti dall'IA



AI Governance
Valutare e rimediare al rischio mentre ti prepari all'uso dell'IA

Directory Security
Scopri e governa Identità agentiche

Identity Security Posture Management
Scansionare e correggere i rischi alla sicurezza dei dati proattivamente

Identity Threat Detection & Response
Proteggere le identità agentiche Da uso improprio

Identity Governance & Administration
Gestione del ciclo di vita di prima classe per ogni identità agentica

Privileged Access Management
Assicurati l'accesso just-in-time delle tue risorse più sensibili ai modelli AI

Oltre il Perimetro: Quando l'Utente incontra la "Shadow AI"

Il Problema: L'illusione della LAN. Molte difese tradizionali (Proxy, Firewall di nuova generazione) funzionano bene finché l'utente è in ufficio o sotto VPN. Ma nel 2026, il lavoro è ovunque.

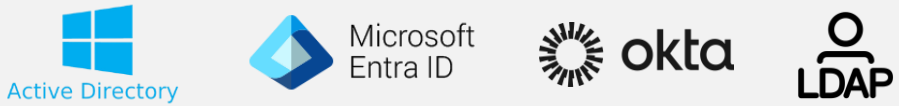
- Il Blind Spot dell'Endpoint: Quando l'utente opera dal laptop di casa o in mobilità senza protezione sull'endpoint, il browser diventa un'autostrada senza caselli verso ChatGPT, Claude o Gemini.
- La "Tentazione" dell'Efficienza: Il dipendente non vuole fare danni, vuole solo "pulire un codice", "riassumere un verbale" o "analizzare un Excel". Senza un controllo granulare sul laptop, il DLP tradizionale fallisce perché non vede il contenuto del *form* web o del *prompt*.
- La Vulnerabilità Identitaria: Un utente con alti privilegi (Admin/Dev) che opera "off-net" è una bomba a orologeria: se le sue credenziali sono compromesse o se commette un errore, l'intera proprietà intellettuale aziendale può finire nel dataset pubblico di un LLM in un click.

Directory Security Journey

Governance / Recovery / PAM

Introducing PingCastle Directory Security

PingCastle™ Directory Security



Unify the Netwrix Directory Security products under the PingCastle brand. Simplify and unify the products to enable expansion through a cohesive suite experience. **All built natively on top of the 1Secure platform.**

Assess	Formerly PingCastle
Monitor	With Netwrix Auditor
Manage	Directory Manager/GroupID
Protect	Threat Manager/Prevention
Recover	Identity Recovery

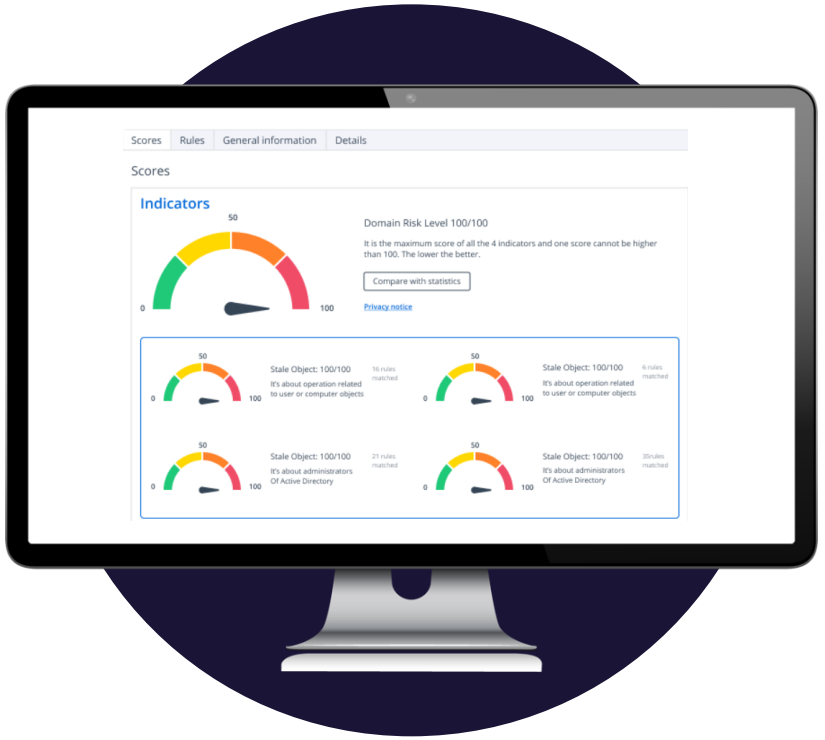
Netwrix PingCastle

A lightweight AD and Entra ID security assessment tool trusted by thousands of organizations globally

Rapidly Identify Risks
Get a comprehensive view of the risks across your AD and Entra ID. Leverage MITRE ATT&CK™ and ANSSI mappings with risk scoring to focus security efforts effectively.

Close security gaps
Reduce your AD attack surface by implementing targeted remediation strategies. Follow our step-by-step recommendations, addressing high-risk vulnerabilities first to strengthen your identity security posture.

Monitor and Improve
Run Netwrix PingCastle on a scheduled basis across domains to detect new risks and trusts. Track progress and security score improvements to ensure ongoing AD protection.



PingCastle Features

Free community edition

- AD health check report
- Risk remediation guidance
- AD Map (attack path visibility)

Paid (Enterprise)

Everything in PingCastle community edition plus

- Advanced report (health check report + AD security maturity assessment and MITRE ATT&CK® coverage assessment)
- Risk remediation tracking
- Historical data and trend analysis
- Scheduled, automated scans
- Multiple domain support
- Configurable authentication
- RBAC

Scan to view a sample PingCastle report

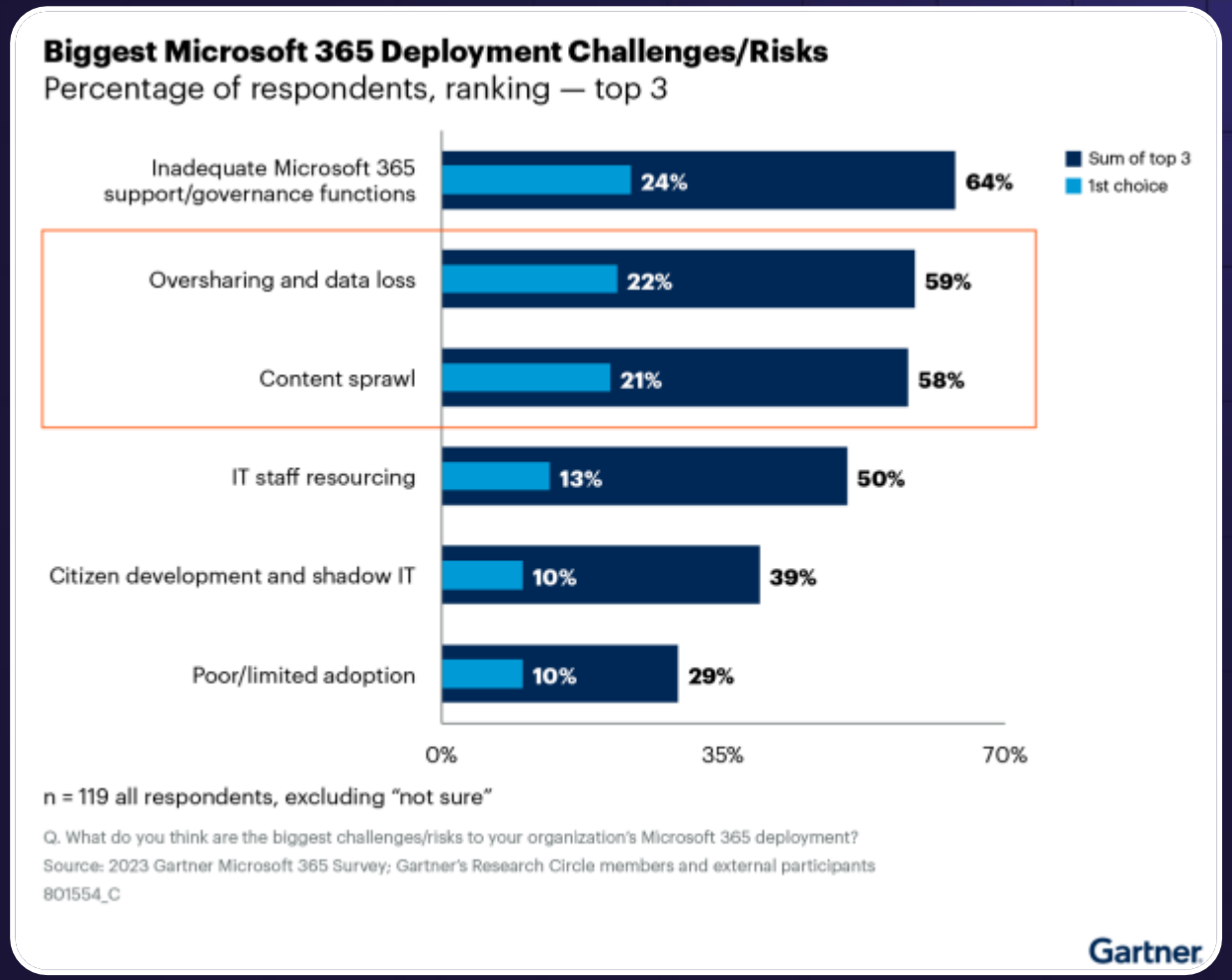
Available on-prem and as a SaaS (part of 1Secure ITDR)

L'eccesso di condivisione è un problema

La maggior parte delle identità ha troppi permessi

Solo l'1% dei permessi concessi viene effettivamente utilizzato

>50% delle identità sono super admin, il che significa che hanno accesso a tutti i permessi e risorse.



Perché Netwrix?

Centro di controllo a 360°

Visibilità unificata e controlli di sicurezza coerenti su cloud, on-premises e ambienti ibridi, offrendo una bonifica automatizzata guidata dall'IA.

ROI veloce

Inizia a sfruttare il tuo investimento fin dall'inizio e ottieni un ritorno sull'investimento in giorni, non in mesi.

Sicurezza dei dati incentrata sull'identità

Le soluzioni Netwrix colmano il divario tra la sicurezza dei dati e quella dell'identità, rendendo più facile rilevare i rischi e neutralizzare le minacce.

Prevenzione proattiva

Correla automaticamente i rapporti sullo stato attuale e i cambiamenti per comprendere i rischi in evoluzione e agire prima che diventino violazioni.

Data Security Posture Management – Come?

01
DISCOVER

Discover dati sensibili, regolamentati e mission-critical.

02
ASSESS

Identifica, assegna priorità e **risolvi** i rischi e le lacune di sicurezza prima di una violazione.

03
PROTECT

Controlla l'accesso alle informazioni sensibili, previeni la perdita di dati e mantienile sempre al sicuro.

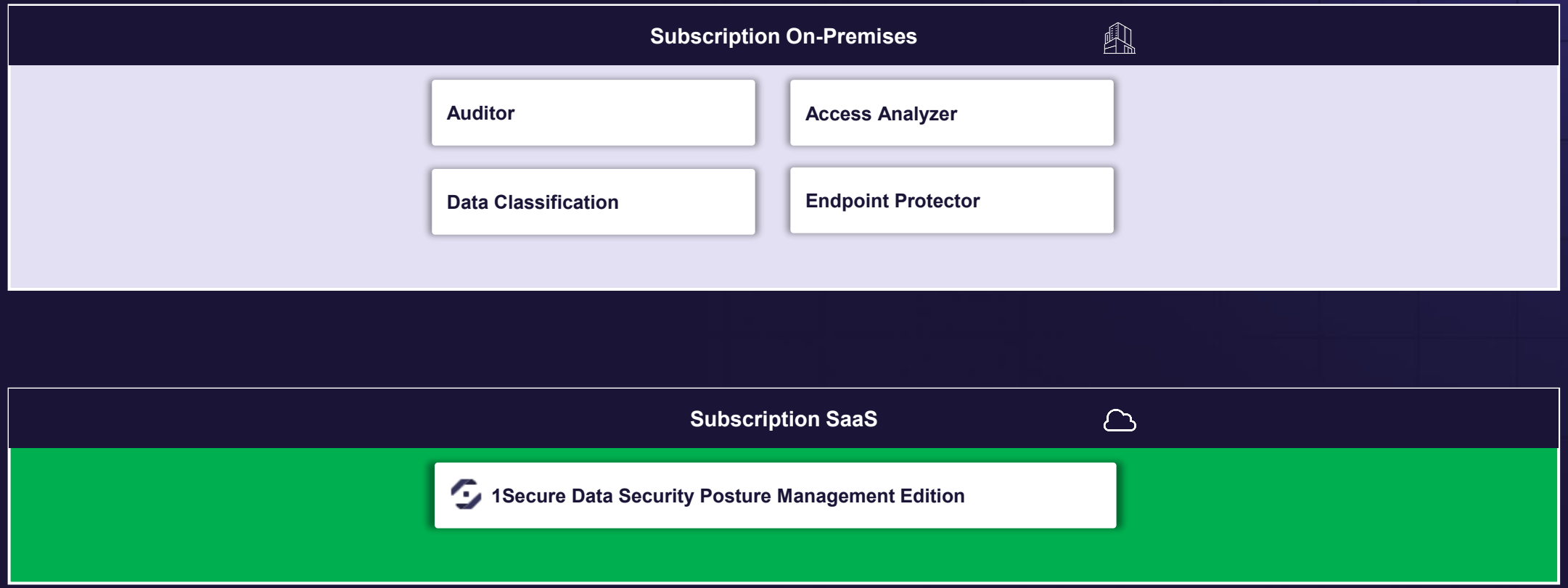
04
DETECT

Rileva comportamenti sospetti per accelerare le indagini e la risposta

05
INVESTIGATE

Analizza gli incidenti di sicurezza e **implementa** le lezioni apprese per rafforzare i dati.

Data Security Posture Management



Netwrix Auditor

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

Netwrix Data Classification

- Identifica e blocca le informazioni sensibili
- Sbarazzati dei dati non necessari per ridurre la superficie di attacco
- Soddisfa i requisiti di privacy e conformità

Netwrix Endpoint Protector

- Facilità d'uso grazie al supporto multi-OS
- Protezione continua in tempo reale, anche offline
- Controllo granulare dei dispositivi approvato dall'amministratore

Netwrix 1Secure

Proteggiti dai rischi di identità e accesso ai dati

Accelera il rilevamento e la risposta agli incidenti

Valuta e mitiga i rischi con informazioni utili

Ottimizza il tuo investimento con la distribuzione SaaS istantanea

netwrix

Demo

netwrix

ACCELERATE

Questions ?

Venite a trovarci al nostro Stand!