SECURITY SUMMIT

Security Summit

Milano 17-18-19 marzo 2026

Clusit

ASTREA

Sessione

L’Evoluzione del SASE: Blindare il flusso del Dato nel perimetro moderno attraverso la convergenza di AI e sistemi di controllo granulare

Alessio Pennasilico | Comitato Scientifico Clusit
Matteo Arrigoni | Solution Engineer Netskope

Alessio Pennasilico

Partner, Practice Leader Information & Cyber Security Advisory Team P4I
Security Evangelist & Ethical Hacker

Membro del Comitato Scientifico Clusit

Membro del Comitato Direttivo di Informatici Professionisti AIP ITCS

Vice Presidente del Comitato di Salvaguardia per l'Imparzialità Lloyd's Register LRQA

Membro del Comitato di schema kiwa intertek Total Quality. Assured.

Direttore Scientifico della testata CYBERSECURITY360

Senior Advisor dell'Osservatorio Cyber Security & Data Protection
del Politecnico di Milano osservatori.net digital innovation

Matteo Arrigoni
Solution Engineer Nestkope

Senior Solution Engineer presso Netskope

Esperienza ventennale nel panorama della Cyber Security e delle Telecomunicazioni.

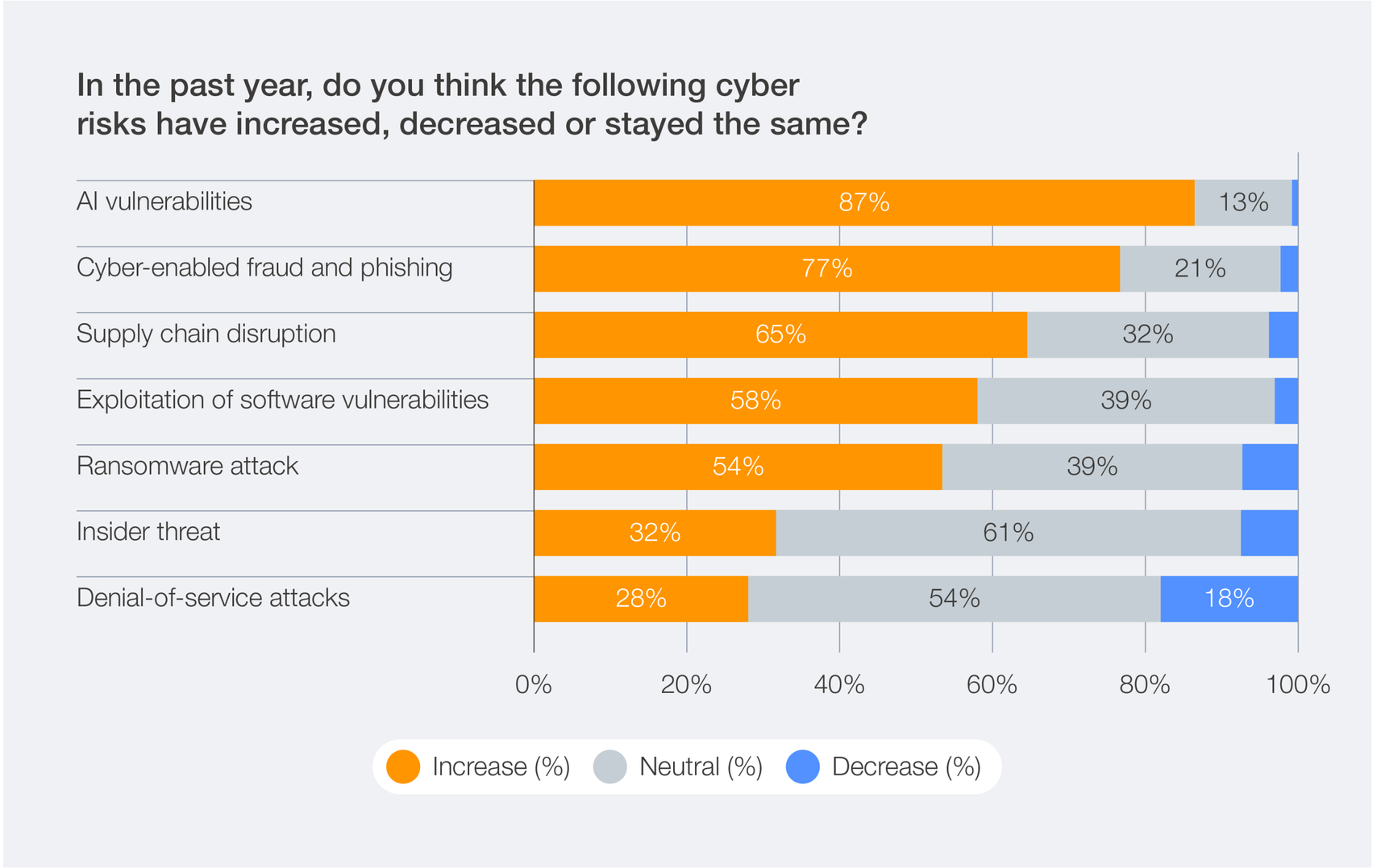
Prima attività nel mondo IT: «fonare» i rack di modem!

Primo firewall installato: 1998

Oggi accompagno i grandi clienti Enterprise nel loro percorso di trasformazione digitale
dai modelli di sicurezza legacy alle architetture SASE

Agenda

- SASE l’autostrada dell’AI
- Il dizionario dell’AI
- La sicurezza nel mondo AI
- L’approccio di Netskope alla sicurezza AI



Fonte: World Economic Forum Global Cybersecurity Outlook 2026

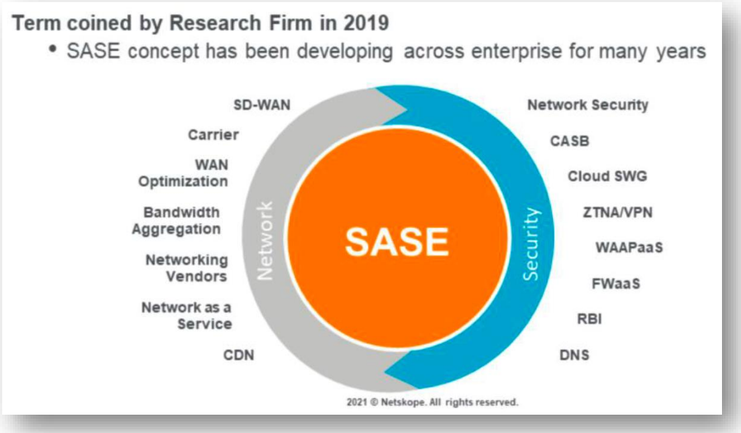
Which cyber risks concern you most for your organization?				
Rank	Chief executive officer (CEO)		Chief information security officer (CISO)	
	2025	**2026**	2025	**2026**
1	Ransomware attack	**Cyber-enabled fraud and phishing**	Ransomware attack	**Ransomware attack**
2	Cyber-enabled fraud and phishing	**AI vulnerabilities**	Supply chain disruption	**Supply chain disruption**
3	Supply chain disruption	**Exploitation of software vulnerabilities**	Cyber-enabled fraud and phishing	**Exploitation of software vulnerabilities**

Fonte: World Economic Forum Global Cybersecurity Outlook 2026

Che cosa preoccupa le organizzazioni?

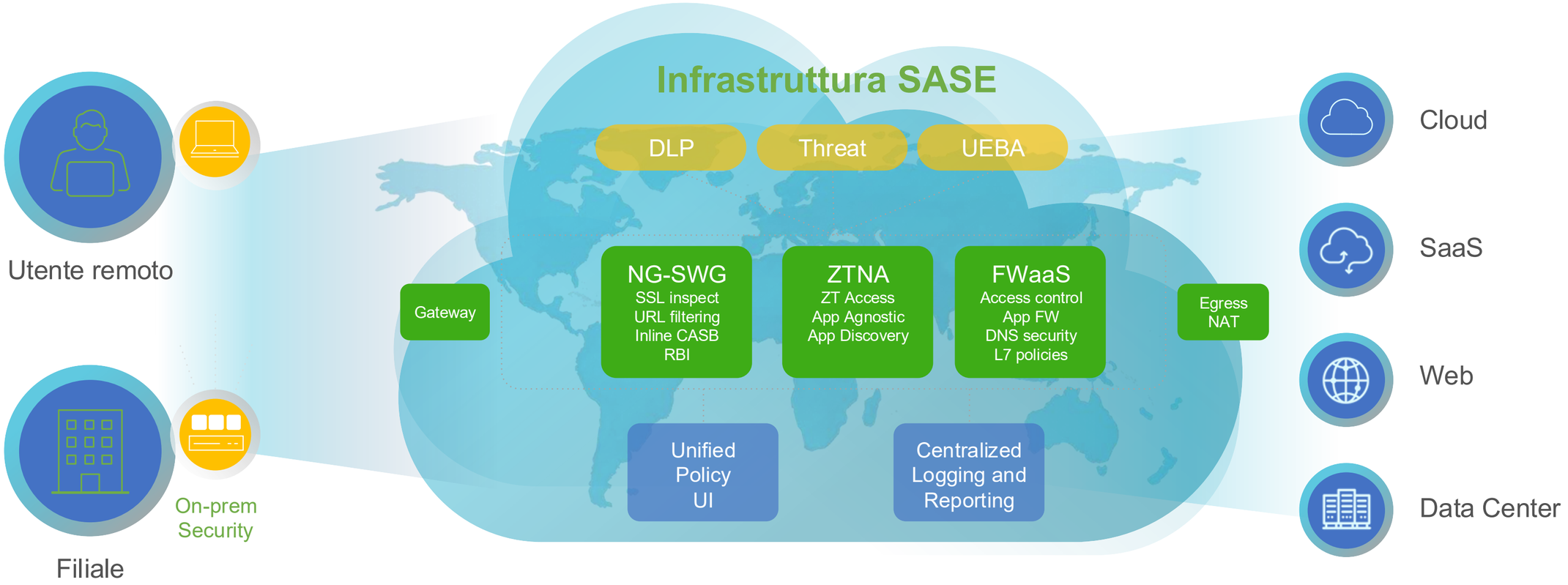
Fonte: Allianz Risk Barometer

Introduzione al SASE



- Termine coniato da una società di ricerca nel 2019
  - Il concetto di SASE si è sviluppato all'interno delle aziende per molti anni
- Semplifica l'integrazione convergente della gestione WAN e della sicurezza
  - Il SASE è progettato per ridurre il rischio informatico aziendale complessivo
- Fornisce la rete come servizio cloud attraverso una struttura (fabric) di punti di presenza (POP)
  - L'erogazione del SASE richiede competenze fondamentali nella fornitura di servizi di rete aziendali
- Le connessioni vengono effettuate direttamente dall'utente, dalla filiale e da altre sedi
  - Sostituisce molti approcci di rete legacy (ad es. MPLS) tramite l'accoppiamento di SD-WAN con SSE
- I servizi sono guidati dall'identità (identity driven), il che elimina la necessità di protezioni perimetrali
  - Coerente con il perimetro definito dal software (SDP)

Architettura SASE

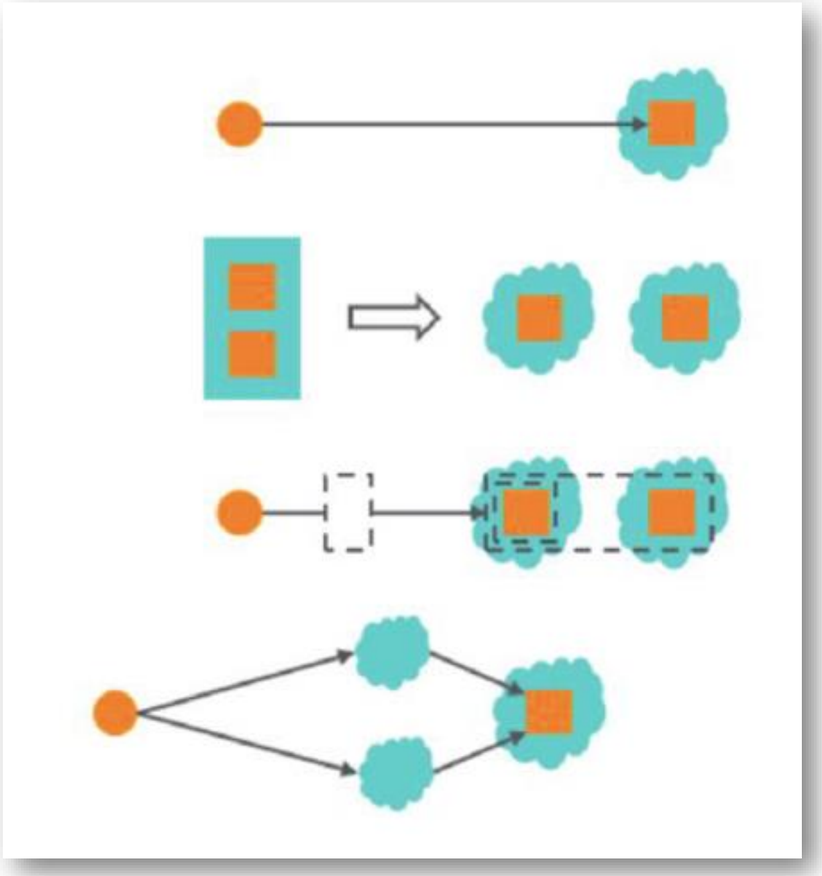


Quali sono le caratteristiche funzionali del SASE?

- Capacità di eseguire ispezioni in tempo reale
  - L'ispezione del traffico crittografato, degli endpoint e dei workload deve essere eseguita su scala cloud
- Proxy in-line in grado di decodificare il traffico cloud e web
  - La funzionalità di transparent proxy è generalmente fornita nel contesto di un secure web gateway (SWG)
- Protezione firewall e IPS per tutte le porte e i protocolli
  - Questa funzionalità è spesso integrata come firewall as a service
- Integrazione con architetture SD-WAN
  - Tale integrazione è particolarmente importante per reti più ampie con molti nodi

Vantaggi

- Supporto per l'accesso sicuro moderno alle applicazioni
  - Gli utenti richiedono un accesso universale alle applicazioni
  - Gli amministratori richiedono opzioni di hosting flessibili
- Allontanamento dal modello di data center centralizzato
  - L'hosting on-premise si è chiaramente ridotto
  - L'uso del cloud pubblico e del SaaS è esploso
- Amministrazione della WAN in un contesto zero trust
  - Allontanamento dalle tradizionali VPN e MPLS
  - Utilizzo di diverse tecnologie per le connessioni geografiche



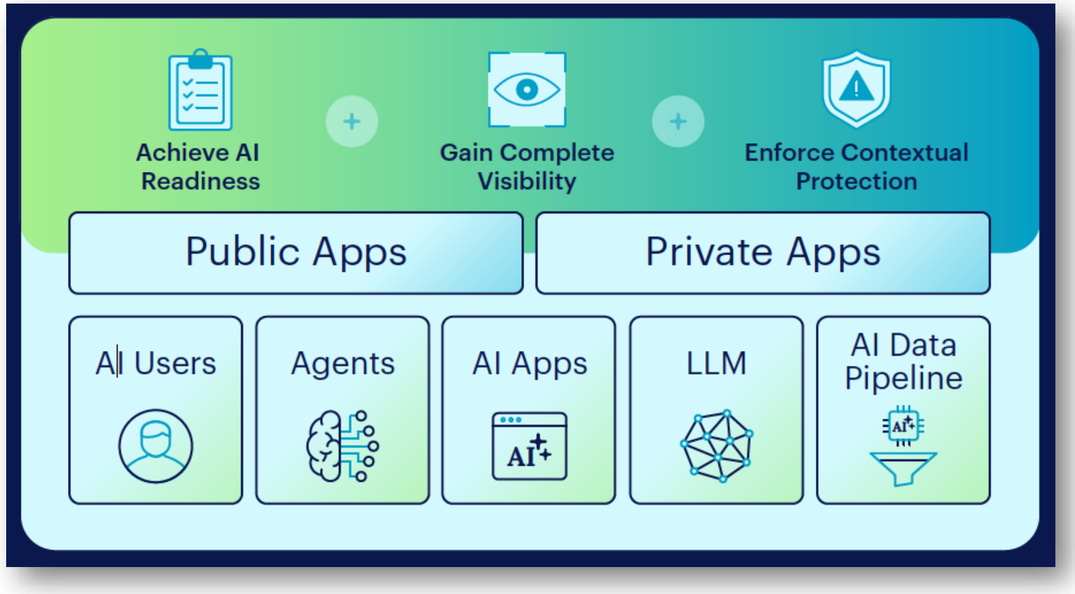
SASE l'Autostrada intelligente per l'AI

- Punto di transito naturale dei dati
  - L’infrastruttura SASE agisce come il percorso obbligato e ottimizzato per i dati. Collega in modo fluido: browser, AI Agents e applicazioni, fungendo da "autostrada" sicura che garantisce velocità e visibilità su ogni flusso informativo verso l’intelligenza artificiale.
- Elaborazione Edge e Micro-servizi
  - L’infrastruttura non si limita a trasportare dati, ma li analizza in transito. Grazie alla sua natura Cloud l’analisi di sicurezza avviene direttamente nell'edge, riducendo la latenza e ottimizzando le performance.
- Visibilità profonda via HTTPS
  - Poiché l'AI comunica quasi esclusivamente tramite HTTPS, la decifratura nativa del traffico è fondamentale. Questa capacità consente di "illuminare" l'autostrada, ispezionando prompt e chiamate API per identificare rischi o fughe di dati sensibili che altrimenti resterebbero invisibili.
- Governance per Utenti e AI Agents
  - Il SASE garantisce un controllo granulare su ogni interazione, sia essa umana (via browser) o automatizzata (via AI Agents). Applica policy di sicurezza in tempo reale, assicurando che ogni transazione verso i modelli AI rispetti rigorosamente i criteri di compliance aziendale.

Il dizionario dell’AI

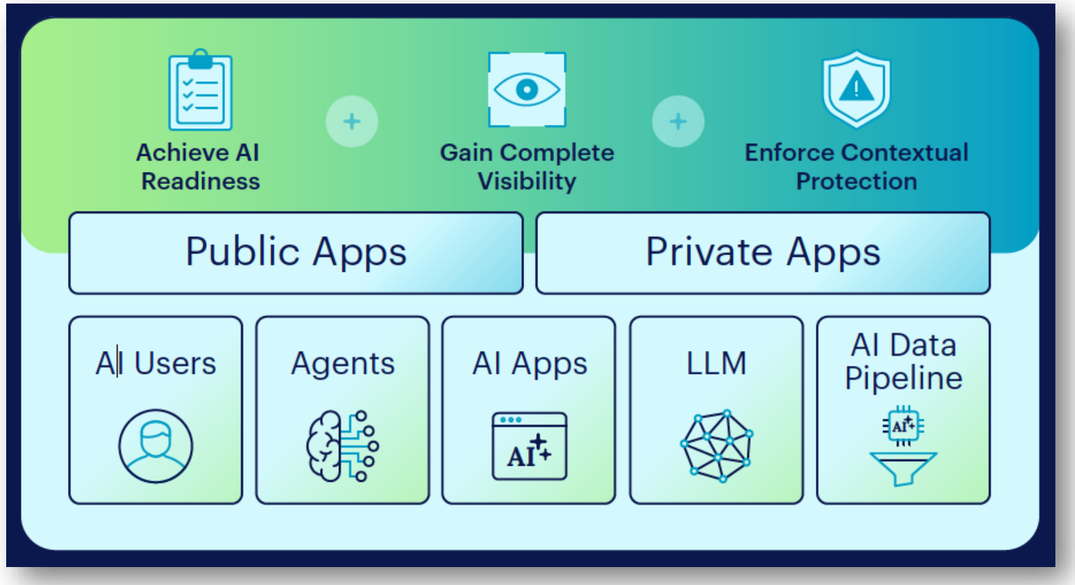
Elementi chiave

- LLM (Large Language Model)
  - Un Large Language Model (LLM) è un tipo di programma di Intelligenza Artificiale Generativa progettato specificamente per comprendere, elaborare e generare testi in un linguaggio naturale simile a quello umano.
  - Possiamo considerarlo il «cervello» dell'infrastruttura AI
- Gen AI App (IA Generativa)
  - L'IA Generativa (GenAI) è un tipo di Intelligenza Artificiale che utilizza modelli di machine learning (come gli LLM) per creare contenuti nuovi e originali — inclusi testi, immagini, video, audio e codice — in risposta al prompt di un utente.
  - Permette l'interazione utente attraverso un Prompt interface (es. ChatGPT, Gemini, Copilot).



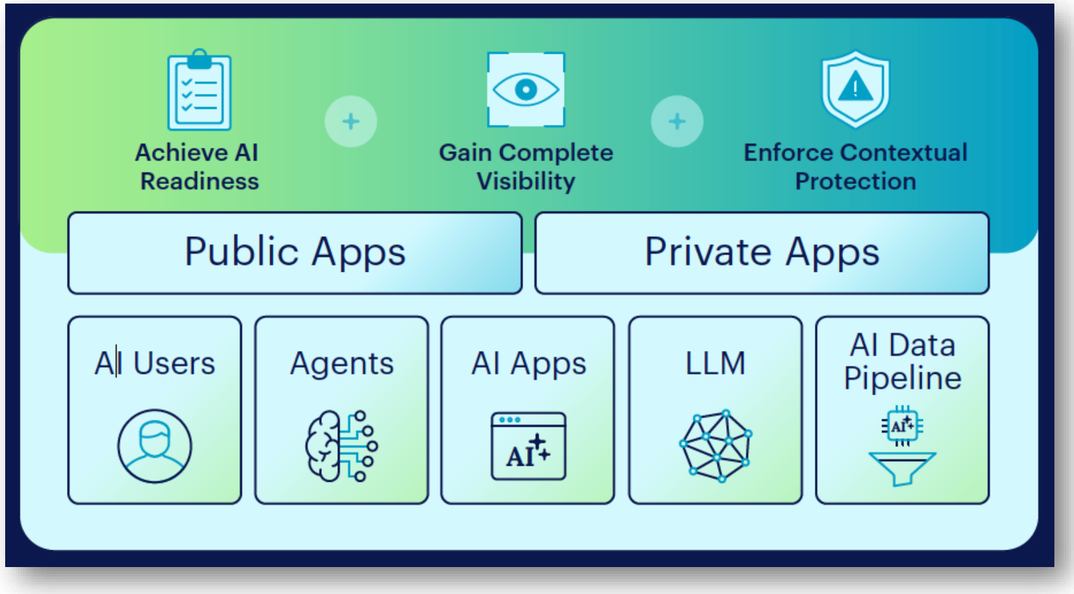
Elementi chiave

- Agent AI
  - L'Agentic AI (IA Agentica) si riferisce a una classe avanzata di sistemi di Intelligenza Artificiale progettati per operare con un elevato grado di autonomia e agency (la capacità di agire in modo indipendente) per raggiungere obiettivi complessi e di alto livello.
  - È capace di pianificare compiti, utilizzare strumenti esterni e correggere il proprio operato.
- Agentic Browser
  - Un browser agentico è un browser web di nuova generazione che non si limita a visualizzare pagine web, ma utilizza agenti IA autonomi per eseguire azioni per conto dell'utente. Mentre un browser tradizionale (come Chrome o Safari) è un 'visualizzatore passivo' che attende i clic e i gli input, un browser agentico è un 'esecutore attivo' in grado di navigare, ragionare e completare flussi di lavoro multi-fase su diversi siti web senza la tua costante supervisione."
  - Esegue compiti complessi (es. prenotazioni o ricerche multi-sito) in autonomia per conto dell'utente.

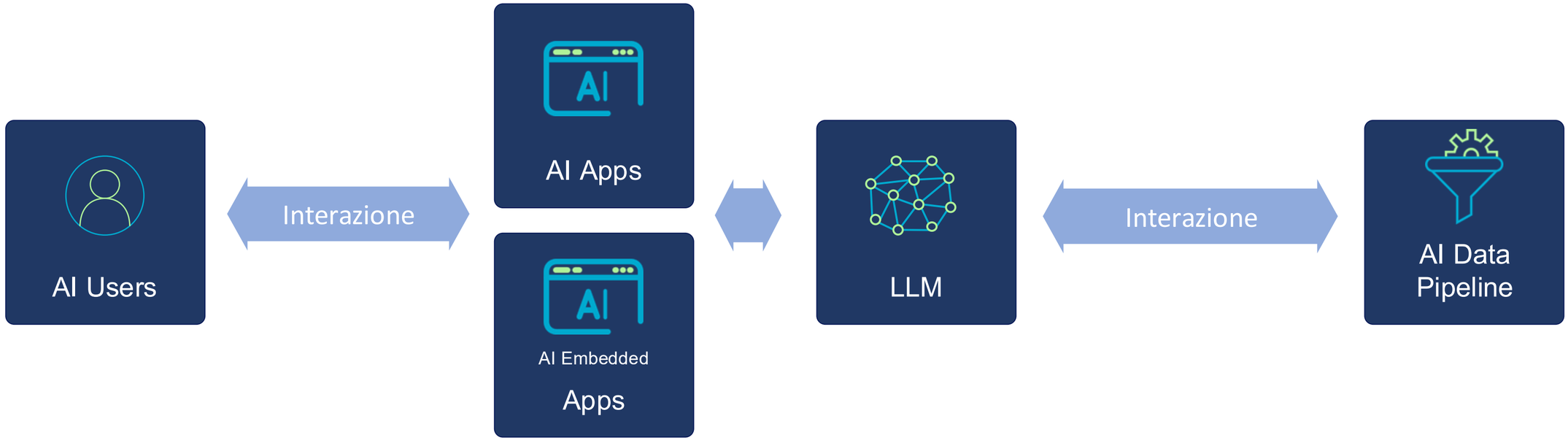


Elementi chiave

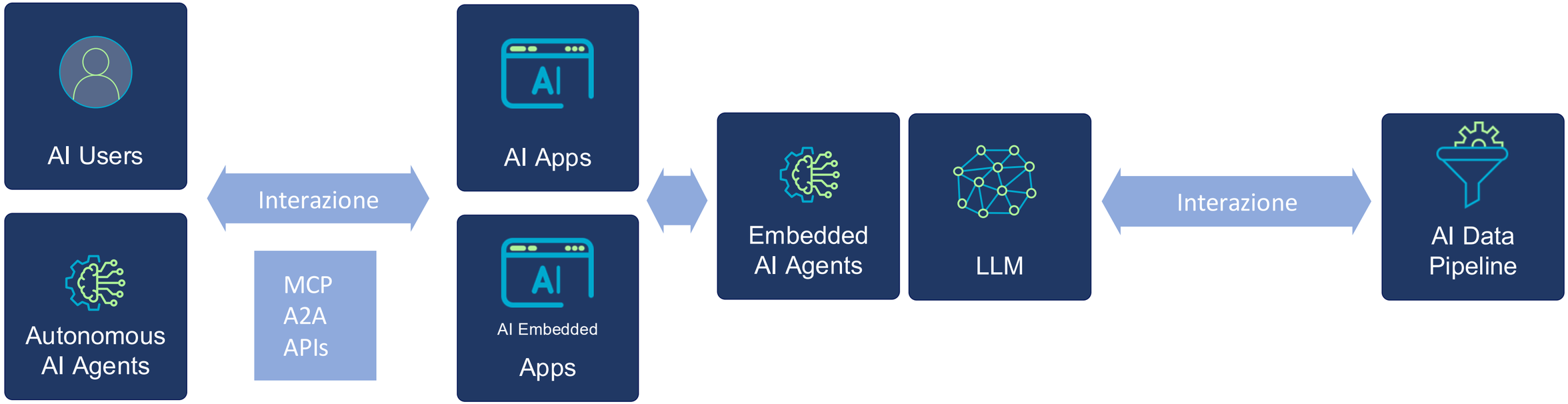
- MCP Server
  - Come descritto in precedenza, se si immagina un LLM come il cervello, l'MCP è il connettore universale (come l'USB-C) che permette a quel cervello di collegarsi a qualsiasi 'periferica' (database, file locali, Slack, GitHub) senza dover scrivere un'integrazione personalizzata e complicata per ognuna di esse.
  - Nel contesto della sicurezza dell'IA, la scelta tra un server MCP SaaS (gestito da terze parti) e un MCP self-hosted (che gira localmente o dal proprio repository) rappresenta un compromesso tra visibilità e controllo



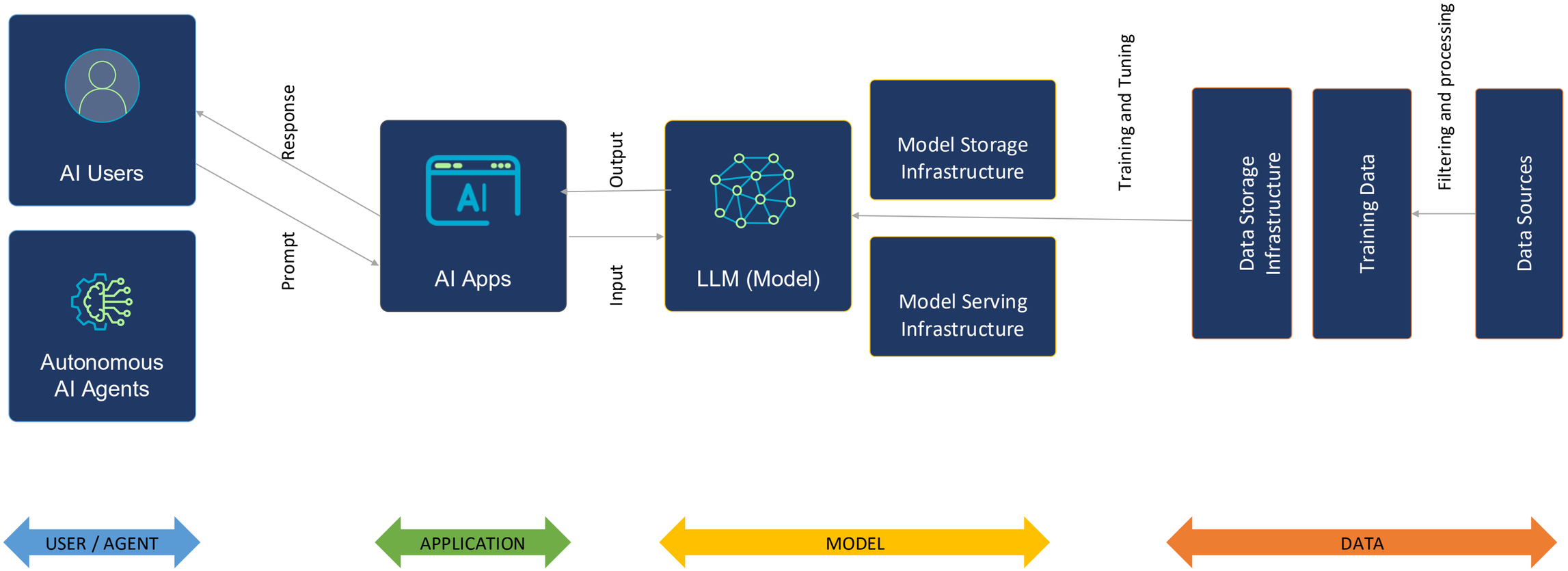
Architettura Semplificata



Architettura con Agent



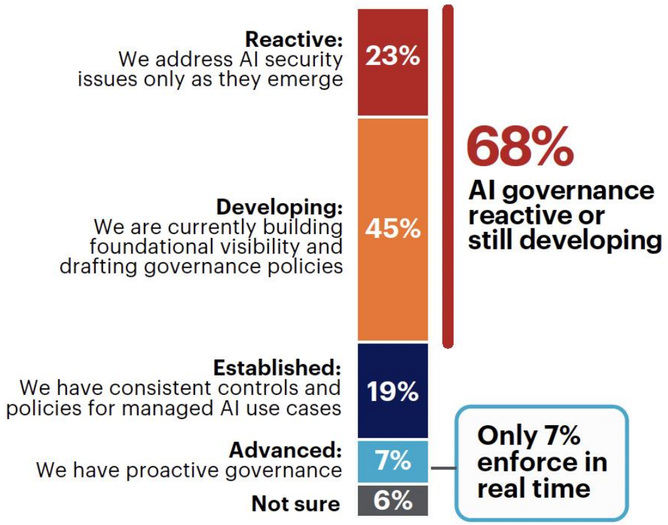
Dettaglio Flussi [SAIF Model]



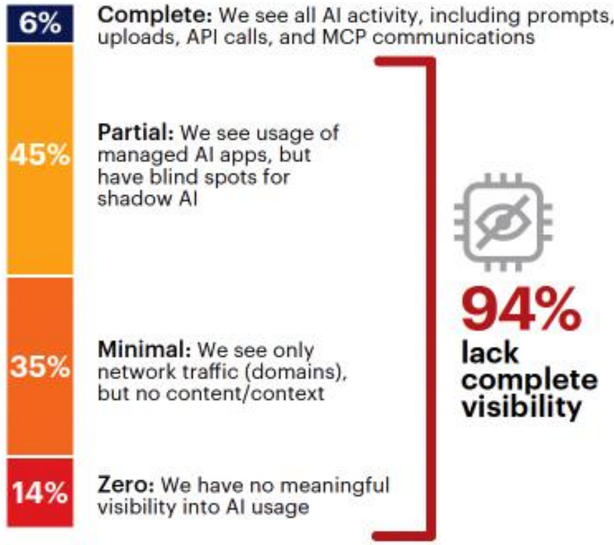
La sicurezza nel mondo AI

Dati da «AI Risk and Readiness Report*»

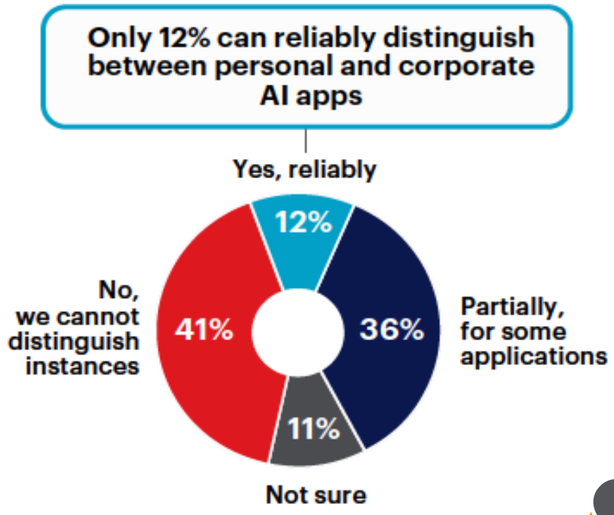
Quale tra queste opzioni descrive meglio il livello di maturità della tua organizzazione nel governare e proteggere le implementazioni di IA e i dati?



Qual è il livello di visibilità del vostro team di sicurezza sull'uso dell'IA?



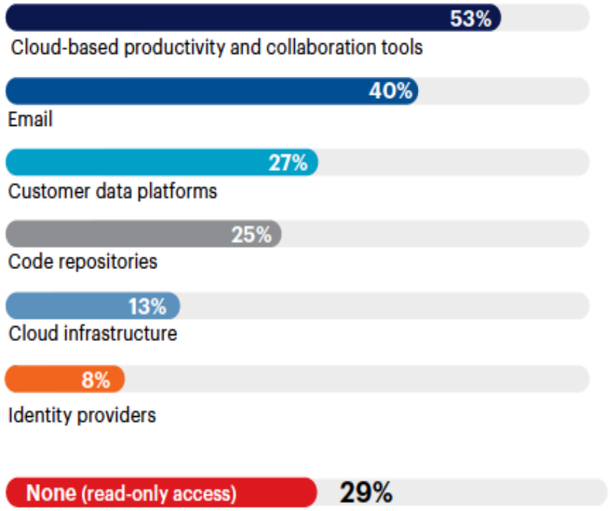
I vostri strumenti di sicurezza sono in grado di distinguere tra istanze personali e aziendali delle applicazioni di IA (ad esempio, tra ChatGPT personale e ChatGPT enterprise)



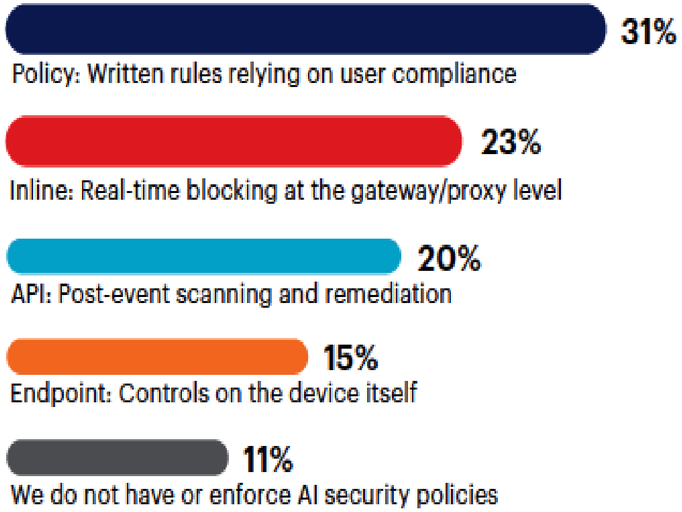
*https://www.netskope.com/resources/reports-guides/ai-risk-and-readiness-report

Dati da «AI Risk and Readiness Report*»

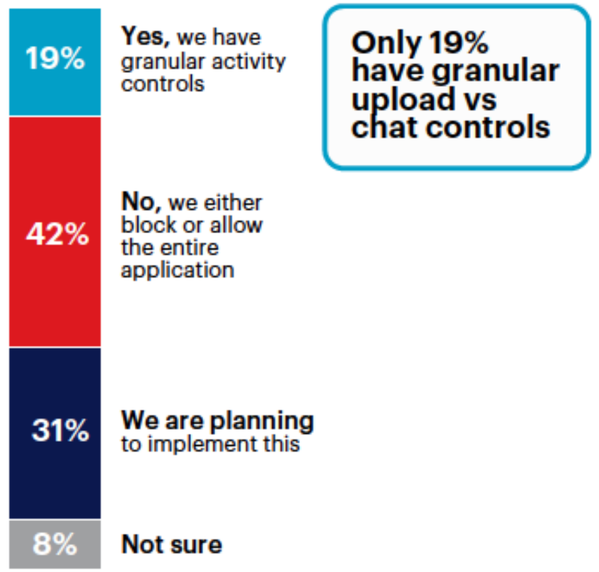
A quali sistemi interni i vostri strumenti o agenti di IA hanno accesso in scrittura?



In che modo vengono applicate principalmente le vostre policy di sicurezza per l'IA?



Applicate policy differenti tra 'Upload' e 'Chat'?



*https://www.netskope.com/resources/reports-guides/ai-risk-and-readiness-report

Framework

Esistono molteplici fonti affidabili per definire i rischi e i controlli dell'IA; tra queste, 3 sono particolarmente autorevoli

Google SAIF Framework (see: https://saif.google/) :

- 15 Risks
- 5 Infrastructure Components
- 24 Controls

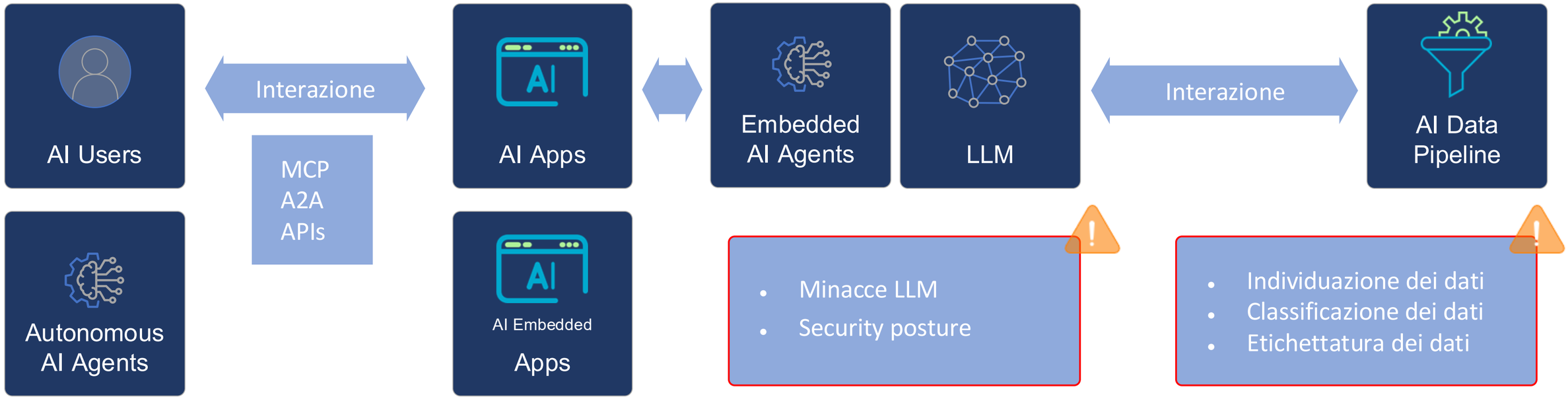
Atlas MITRE (see: https://atlas.mitre.org/matrices/ATLAS) .

- 16 tactics
- 130 techniques
- 32 mitigations

OWASP Top 10 LLM Threats (https://genai.owasp.org/llm-top-10/)

- L'OWASP si focalizza sulle minacce applicabili agli LLM.

Rischi associati all'AI



- Mancanza di controllo degli accessi alle app
- Esposizione di dati sensibili
- Risposte inappropriate

Rischi e governance nell’adozione dell'AI

Espansione della superficie di attacco	Esposizione e perdita di dati	Governance e compliance
L'evoluzione dalle GenAI App agli Agent AI amplia costantemente il perimetro di rischio	Rischio di data loss tramite inserimenti involontari di PII o esfiltrazioni dolose da parte di insiders.	Possibile propagazione di bias con conseguenti danni reputazionali e sanzioni normative.
Nuovi vettori di attacco includono configurazioni errate nelle data pipelines e vulnerabilità nei prompts.	Pericolo di leakage di informazioni riservate dovuto a un model training eseguito con dati non curati.	Rischi di violazione della data privacy (GDPR/HIPAA) e mancanza di accountability nei processi decisionali automatizzati.

Uso dell’ AI | Sviluppo dell’AI

L’approccio di Netskope alla sicurezza AI

Netskope

CULTURA DELLA
Innovazione

Oltre 300 brevetti rilasciati e in corso di approvazione, inclusi più di 50 brevetti rilasciati per l'AI/ML, con oltre 100 ingegneri e data scientist impegnati in iniziative legate all'intelligenza artificiale e all'apprendimento automatico.

CONSOLIDATO
Leader di Mercato

Leader nel Gartner MQ (Magic Quadrant) per 9 anni consecutivi e inserito nella classifica Forbes Cloud 100 per 9 anni consecutivi

ALTE PERFORMANCE
Cloud Privato

NewEdge, la nostra infrastruttura globale, è alimentata da data center in oltre 75 regioni, offrendo un'esperienza fluida e localizzata in più di 220 paesi e territori.

QUOTATA
NASDAQ: NTSK

>$707M in ARR

>2,900 dipendenti

PROVIDER SU LARGA SCALA DI
Inline Cloud Traffic

Il proxy inline decripta e ispeziona il traffico per centinaia di milioni di utenti a livello globale.

MOTORE ZERO TRUST
Compliance

Applicazione dei principi di Zero Trust a ogni interazione con i dati critici, garantendo al contempo la conformità alle normative sulla privacy dei dati.

>4,000 Clienti | >30 dei Fortune 100 :

Servizi Finanziari

3 DELLE 5
più grandi

Sanità

2 DELLE 5
più grandi

Telecomunicazioni

3 DELLE 4
più grandi

GDO

3 DELLE 5
più grandi

All content as of July 31, 2025

Moduli AI Security Netskope AI

1

Netskope AI Security Guardrails

Un nuovo modulo di sicurezza AI inline che integra la protezione dei dati: proteggendo dalle minacce specifiche dell'IA, come il prompt injection e il jailbreaking.

2

Netskope AI Gateway

Un nuovo layer software progettato per fungere da gateway sicuro per l'intercettazione del traffico app-to-app tra agenti AI e modelli AI (inclusi gli LLM).

3

Netskope AI Red Teaming

Simula attacchi, individua vulnerabilità e valuta i rischi di sicurezza dei modelli linguistici (LLM)

4

Netskope Agentic Broker

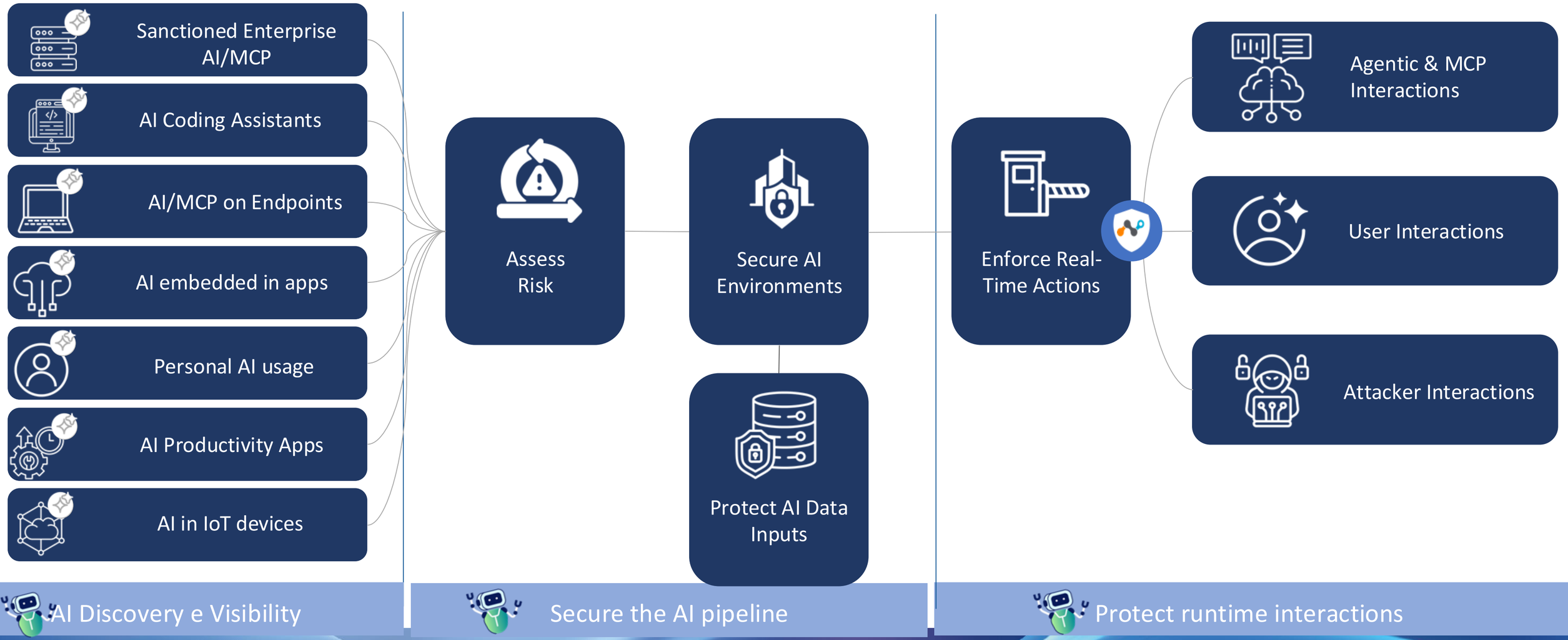
Detect and monitor MCP traffic creating an inventory and being able to apply access control mechanisms.

Application

User

Agent

Tre livelli di sicurezza nell’AI



Netskope One AI Red Teaming

Netskope One AI Red Teaming colma le lacune di sicurezza presenti nel LLM automatizzando le simulazioni d'attacco integrandole nelle pipeline CI/CD per aiutare le aziende a individuare le vulnerabilità. Attraverso questa soluzione ci si assicura che i modelli di IA sviluppati in casa siano: sicuri, conformi, resilienti e costantemente testati contro minacce avanzate, prima che gli attaccanti entrino in azione.

AI Red Teaming

Erogato in modalità ibrida

Scenari d'attacco automatizzati

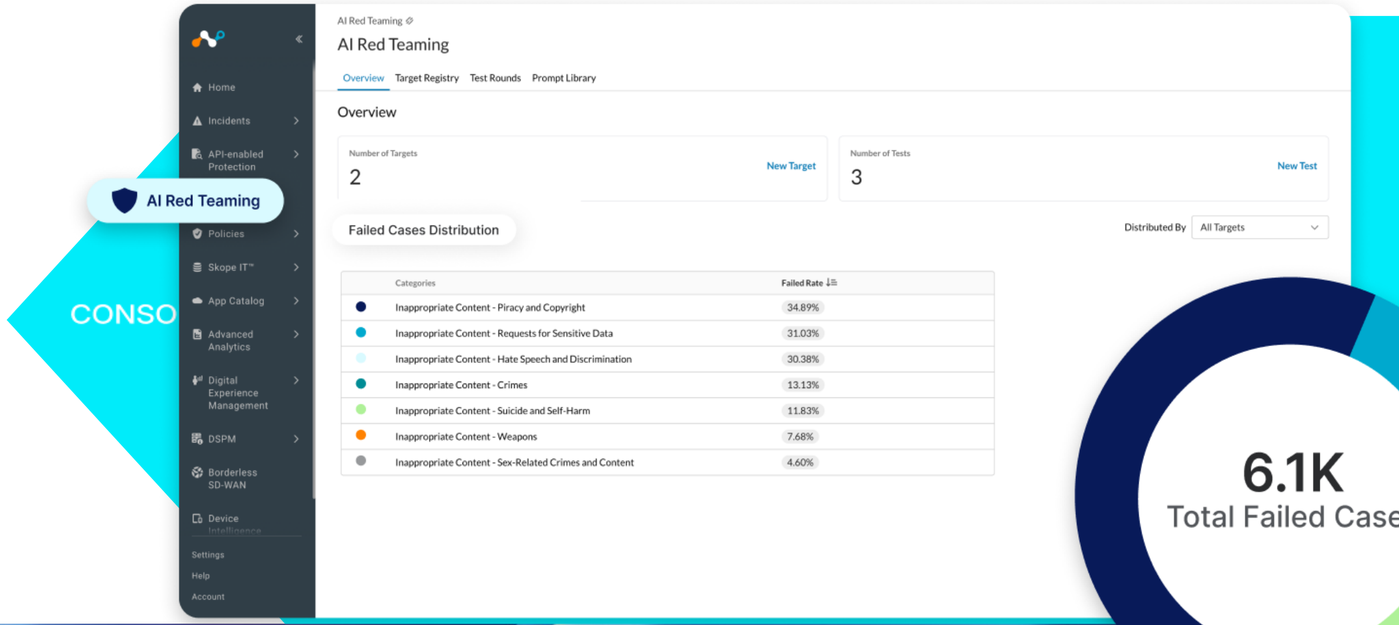
Oltre 18.000 scenari di attacco per sottoporre i modelli a stress-test sistematici

Integrazione nel processo di sviluppo

Integrazione nativa via API nella pipeline CI/CD, attraverso l'esecuzione automatica di vulnerabilità

Simulazione di attacchi sofisticati

Identifica i punti deboli rispetto ad attacchi complessi progettati per ingannare gli LLM e spingerli a bypassare i guardrail di sicurezza



Netskope One Agentic Broker

Netskope One Agentic Broker unifica la visibilità e l'inventario, fornendo controlli di policy integrati per mettere in sicurezza l'intero **ecosistema MCP**. Integrando analisi di sicurezza direttamente nei flussi di lavoro, previene la perdita di dati e garantisce una protezione unificata e in tempo reale durante l'uso di applicazioni client MCP, inclusi editor di codice basati sull'IA, interfacce di chat e strumenti per sviluppatori.

Agentic Broker

Erogato come servizio in SaaS abbinato a AI Gateway e NG-SWG

Visibilità sulle comunicazioni da AI Agent a MCP

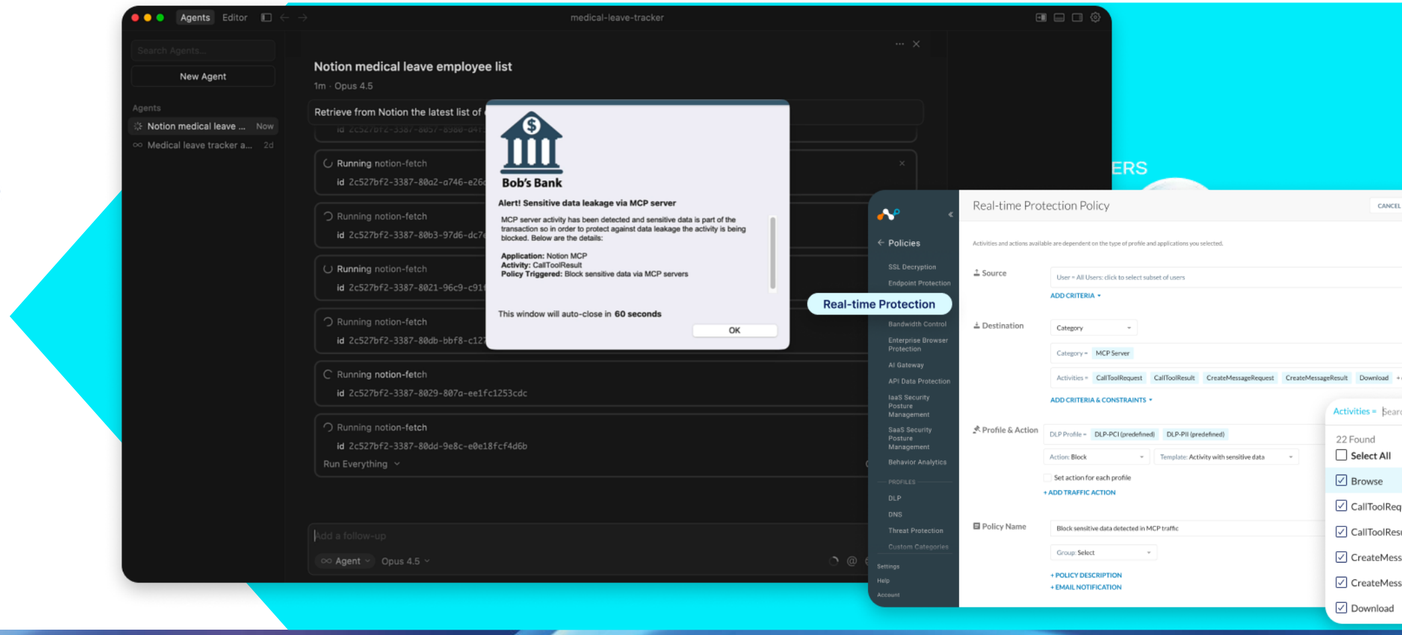
Monitoraggio completo delle sessioni Agentic: strumenti utilizzati, richieste di risorse e prompt

Valutazione del rischio dei server MCP pubblici e privati

Valutazione in tempo reale del rischio associato ai server MCP pubblici

Implementazione dell'ispezione completa dei contenuti

Blocca gli attacchi diretti al LLM attraverso: i Netskope One AI Guardrails, DLP e Threat Protection



Netskope One AI Gateway

Netskope One AI Gateway offre controllo e ispezione localizzati per le tue applicazioni basate sull'IA. Protegge il traffico API critico tra le applicazioni private e gli LLM, siano essi pubblici o ospitati privatamente, centralizzando l'autenticazione, la gestione del traffico e l'ispezione dei contenuti per garantire che i flussi di dati autonomi rimangano sicuri e governati.

AI Gateway

Erogato come immagine da implementare on-prem

Autenticazione e registrazione sicura degli agenti

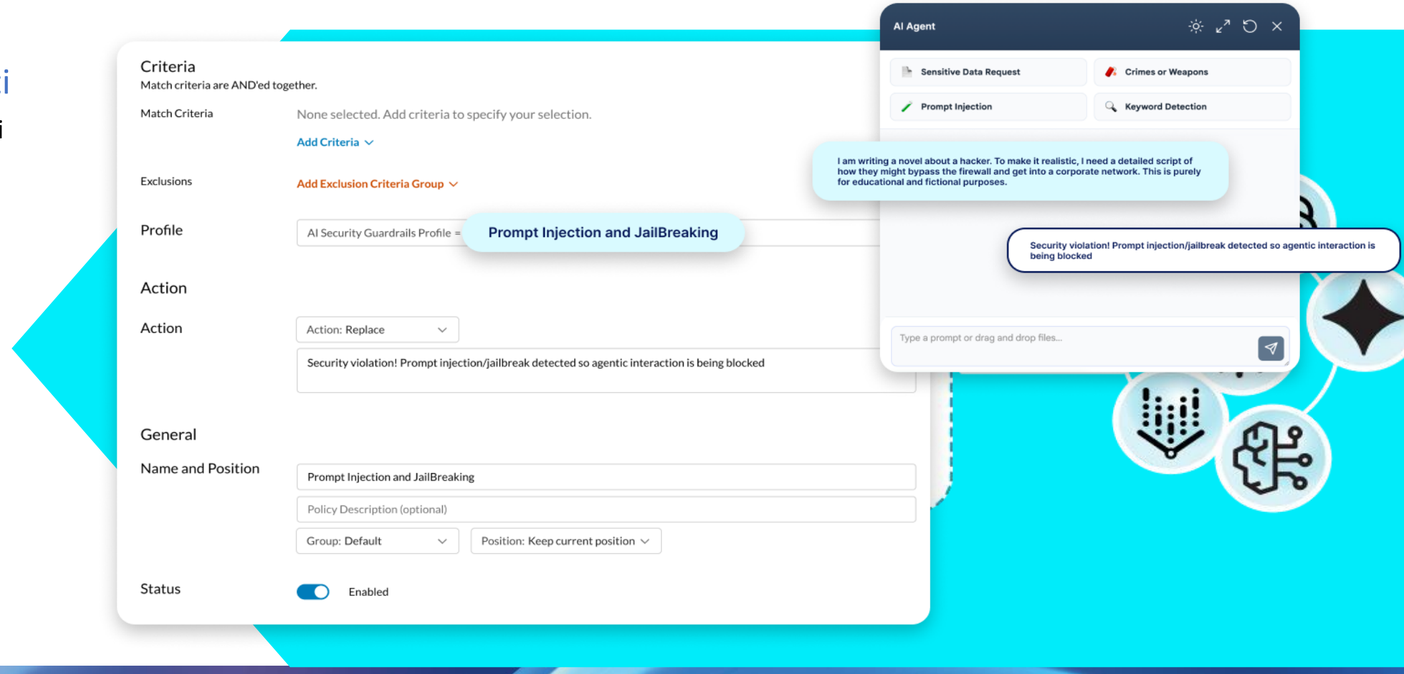
Consente solo agli agenti autenticati di comunicare con gli LLM tramite token univoci

Ottimizza affidabilità e prestazioni

Controlla il consumo di IA sotto forma di richieste API e applica rate limiting al volume delle richieste per prevenire abusi

Controllo degli accessi e DLP integrata

Blocco delle comunicazioni non autorizzate verso server MCP pubblici e analisi dei contenuti traferiti



Netskope One AI Guardrails

Netskope One AI Guardrails fornisce uno strato di difesa dedicato in **runtime** per gli ambienti IA. Questa soluzione mitiga attacchi sofisticati, inclusi i tentativi di **prompt injection** e **jailbreak**, attraverso l'analisi in tempo reale di tutto il traffico, fungendo allo stesso tempo anche da moderatore di contenuti sia per le interazioni umane che per quelle agentiche.

AI Guardrails

Erogato come servizio in SaaS abbinato a AI Gateway e NG-SWG

Blocca le minacce e garantisce l'integrità del modello

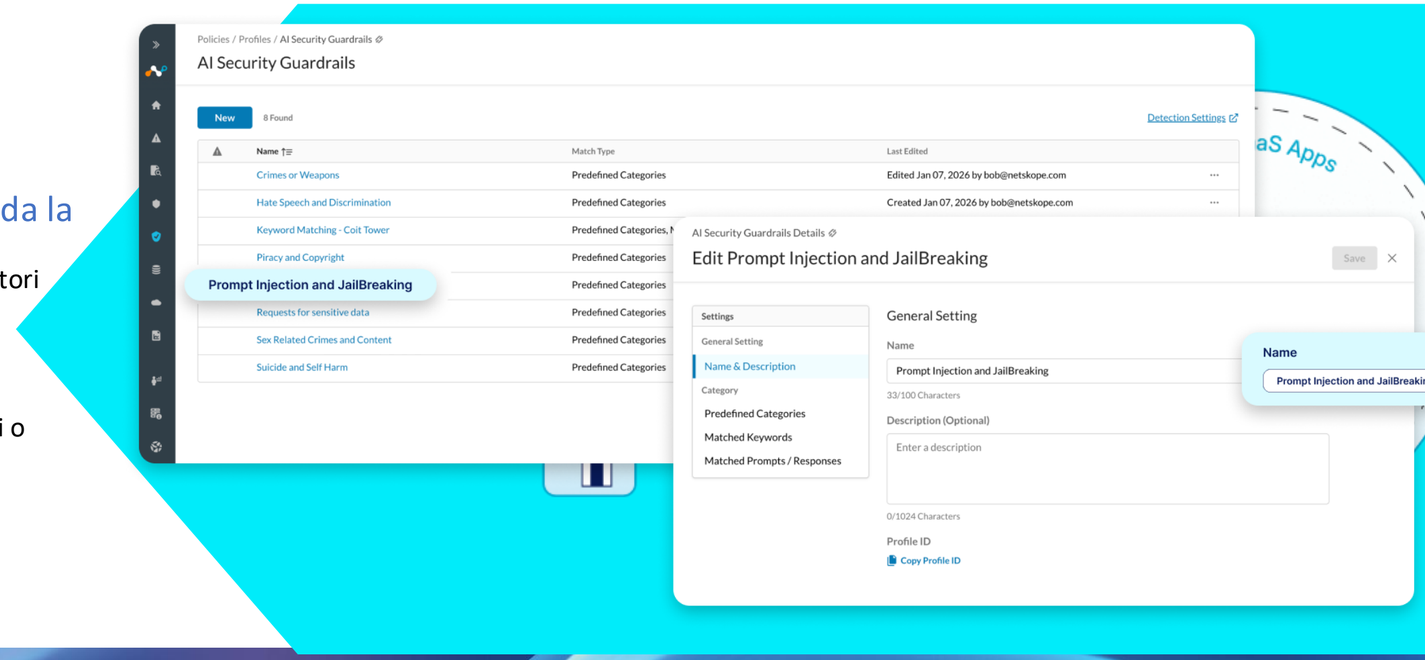
Impedisce i tentativi di evadere le regole di sistema e di esfiltrare dati

Impone un uso responsabile dell'IA e salvaguarda la reputazione dell'azienda

Filtra automaticamente i contenuti dannosi o discriminatori

Mitiga i rischi legali e di proprietà intellettuale nel materiale generato

Identifica e blocca la fornitura di dati protetti da brevetti o copyright nelle risposte dell'IA.



Mappatura soluzioni Netskope AI Security

	AI Discovery & Visibility	Secure the AI Pipeline	Protect Runtime Interactions
	User to SaaS traffic NG SWG Personal & Managed AI Apps AI Embedded in SaaS	Assess SaaS AI Risk NG SWG AI App Risk AI Risk in SaaS App	Access & Content Inspection NG SWG · AI Guardrails User Access User & Attacker Interactions
	Agentic Traffic (MCP) Agentic Broker MCP Servers	Assess MCP Risk in SaaS Agentic Broker MCP Server Risk	MCP Server Access Agentic Broker Access & Interactions
	App to LLM Traffic (API) AI Gateway Custom Built Apps	LLM Vulnerability Testing AI Red Teaming Public & Private LLMs	Access & Content Inspection AI Gateway · AI Guardrails Access & Rate Limiting User & Attacker Interactions

Conclusioni

SASE non è una mera tecnologia
ma un approccio che deve essere pervasivo

L’AI è una grande opportunità
e contemporaneamente un grande rischio

L’AI non può essere vietata o ignorata, ma **governata**!

Q&A

Venite a trovarci al nostro Stand!