



Dalla Shadow AI alla resilienza operativa

Governance & Compliance, AI-powered Prevention e Breach Containment

22 Settembre 2026

WE SECURE YOUR AI
TRANSFORMATION

Dalla Shadow AI alla resilienza operativa



**Antonio
Altamura**
*Director, Sales,
EMEA South
Illumio*



**Fabio
Battelli**
*Enterprise
Security Leader
Deloitte*



**Massimiliano
Bossi**
*Enterprise Sales
Manager Italy
Check Point*



**Giulia
Cabianca**
*Enterprise AI
Security
Advisor
Check Point*



**Paolo
Melchiori**
*Sales Engineer
Check Point*

Un attacco che sembra un'attività legittima

01

Credenziali
legittime
compromess
e

02

Accesso a un
servizio
Shadow AI
non censito

03

Connessione
a dati e
applicazioni
aziendali

04

Escalation e
movimento
laterale

05

Impatto su
funzioni
critiche

“Se l’identità è valida e l’applicazione AI è invisibile, dove inizia il perimetro di sicurezza?”

Dal primo accesso alla crisi operativa

10:02

Utilizzo di
credenziali
legittime

10:04

Accesso a un
servizio AI non
mappato

10:07

Interrogazione
di dati e sistemi
connessi

10:12

Movimento
laterale

10:20

Raggiungiment
o potenziale di
asset critici

**«Se qualcosa entra alle 10:02, cosa può raggiungere alle 10:12?»
«In quale minuto l'evento viene considerato rilevante ai sensi della
normativa DORA?»**

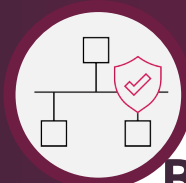
Cyber Resilience Acceleration Program



Governance & Risk Management

Deloitte.

Strategy | Roadmap | DORA | NIS2 |
AI Act | Compliance | Organizational
Readiness



Breach Containment

illumio

Microsegmentation | Zero Trust
Segmentation | Ransomware
Containment | Lateral Movement
Prevention



AI-Powered Prevention

CHECK POINT
SERVICES

AI Defense Plan | AI Network Firewall



Continuous Threat Exposure Management

CHECK POINT
SERVICES

Exposure Discovery | Vulnerability
Prioritization | Attack Path Analysis

Cyber Resilience Acceleration Program



Governance & Risk Management

Deloitte.

Strategy | Roadmap | DORA | NIS2 |
AI Act | Compliance | Organizational
Readiness



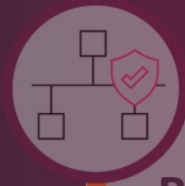
AI-Powered Prevention

AI Defense Plan | AI Network Firewall



Continuous Threat Exposure Management

Exposure Discovery | Vulnerability
Prioritization | Attack Path Analysis



Breach Containment



Microsegmentation | Zero Trust
Segmentation | Ransomware Containment
| Lateral Movement Prevention



La fotografia italiana della GenAI Security



Fonte: Deloitte e Cloud Security Alliance, Lo stato della GenAI Security 2026.

80%

+

Utilizza o
prevede di
utilizzare
GenAI

3%

Ha
raggiunto
un'adozion
e su scala
enterprise

9%

Dei CISO
dichiara
piena
visibilità

2/3

Non ha
una
strategia
strutturat
a di AI
Security

Deloitte.

CSA cloud
security
alliance®

Lo stato della GenAI Security

I CISO italiani alla guida della
nuova frontiera della sicurezza

Lo stato della GenAI Security

La survey e il Programma AI Safety



Partnership Deloitte –
CSA

Deloitte.

La survey è stata realizzata come parte del più ampio programma AI Safety di CSA.



Deloitte ha scelto fin dalle fasi iniziali di contribuire attivamente con i propri **professionisti italiani** ai principali **working group internazionali** di tale programma.



AI Safety
Program

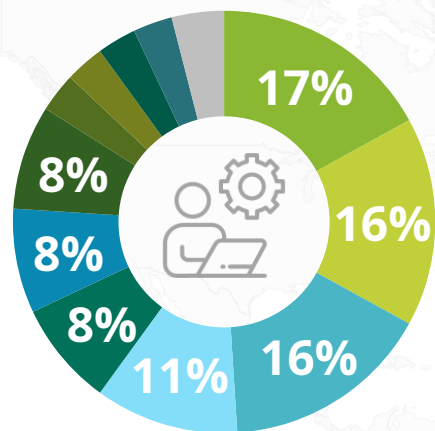
Una **coalizione globale** di **esperti e industry leader** che, attraverso ricerca vendor-neutral, working group e strumenti come l'**AI Controls Matrix**, definisce **standard** e **pratiche concrete** per **guidare** le **organizzazioni** verso un'**AI sicura, responsabile** e **conforme**.



La Survey

Metodologia

17% appartiene al **settore ICT**



- ICT
- Servizi finanziari
- Manifatturiero, costruzioni e automotive
- Settore pubblico / PA
- Energia e utilities
- Intrattenimento, media e comunicazioni
- Trasporti e logistica
- Commercio e retail
- Istruzione e ricerca
- Farmaceutico e biotecnologie
- Telecomunicazioni
- Altro

Focus principale
Italia



100+
aziende

hanno
partecipato alla
Survey

51% dei rispondenti **opera**
principalmente in
Europa

dei rispondenti ha
81% **sede legale** in
Italia

+60%

dell'audience rientra nella
fascia **fra i 1.000 e 50.000**
dipendenti

39%

degli intervistati ha un **ricavo**
annuo > 1 mld €

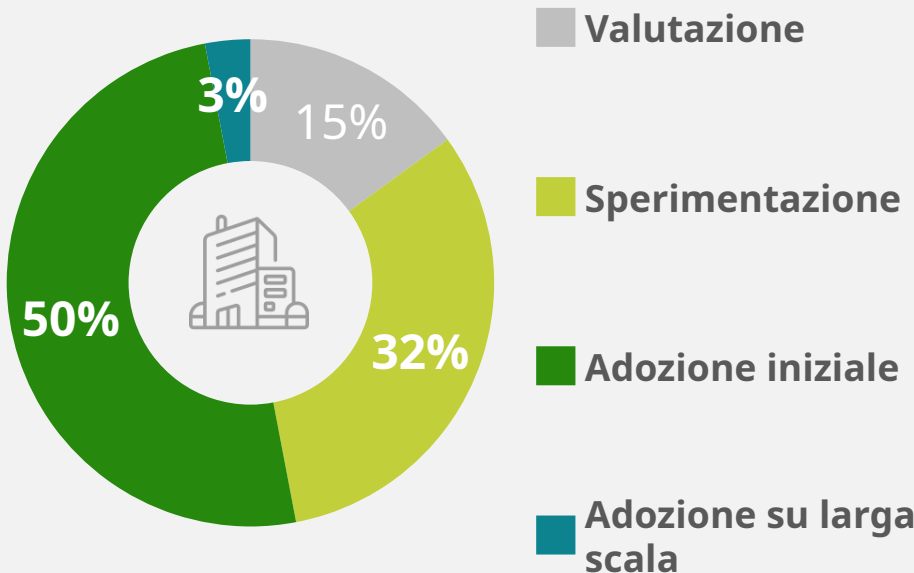
Adozione dell'AI e modelli di governance

Stato di adoption e principali Use Case GenAI



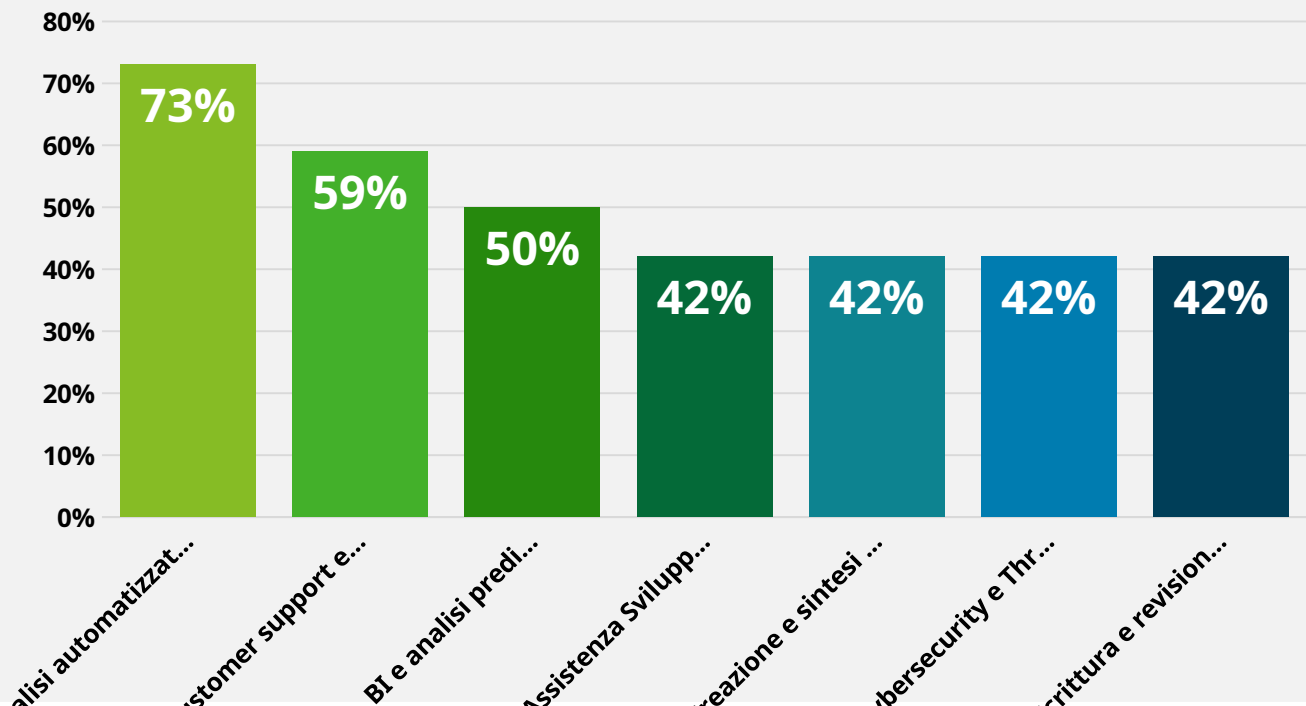
>80% **utilizza o prevede GenAI nel breve periodo.**

Stato di adozione della GenAI



Solo il 3% ha raggiunto un'**adozione su scala enterprise.**

Casi d'Uso GenAI più diffusi



Adozione dell'AI e modelli di governance

L'AI Steering Committee e il ruolo della Security

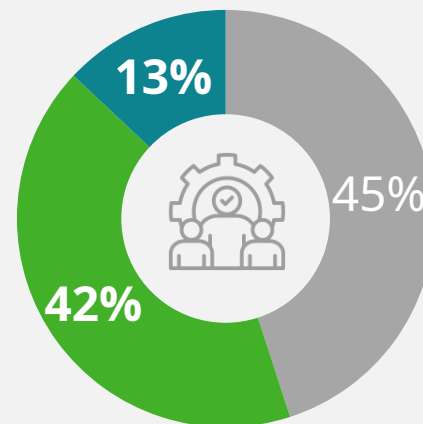


La **Security** è ancora **poco integrata** nella **governance GenAI**, riducendo l'efficacia nella gestione del rischio.

58% non ha un AI **Steering Committee** o **non** vi **coinvolge** il **CISO**.

25% delle **organizzazioni non coinvolge** sin da subito la **sicurezza AI** nei progetti di **sviluppo**.

Livello di adozione dell'AI Steering Committee

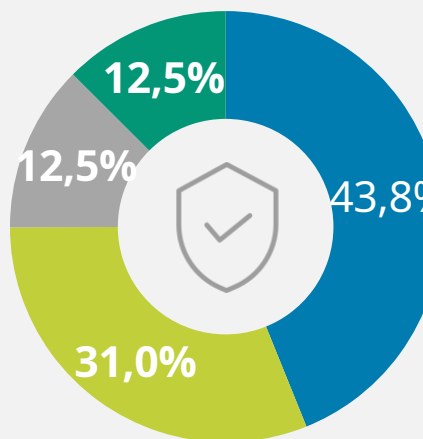


■ Non presente

■ Presente e include la funzione Security

■ Presente ma non include la funzione Security

Livello di coinvolgimento della Security



■ On-demand

■ Formale

■ Nessuno

■ Reattivo

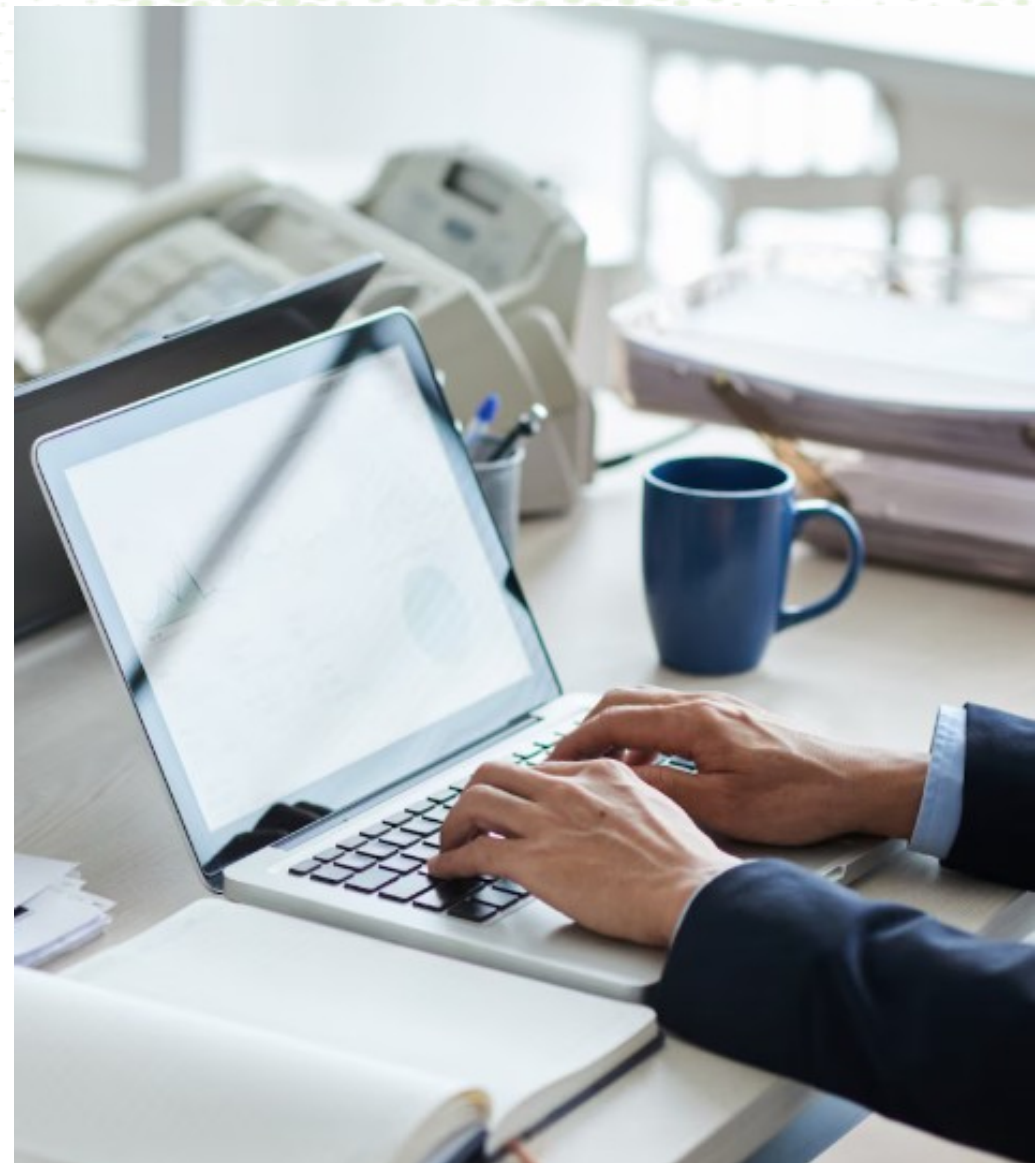
Percezione e gestione del rischio AI

Come le organizzazioni stanno gestendo i rischi AI

Nonostante le organizzazioni percepiscano i **rischi GenAI** con una **severità media** di **3.6/5**, nel **panorama italiano** **l'attenzione** continua a **concentrarsi** prevalentemente sui **domini cyber tradizionali**.

Solo il **9%** dei **CISO** dichiara una **piena visibilità** sulle iniziative **GenAI**.

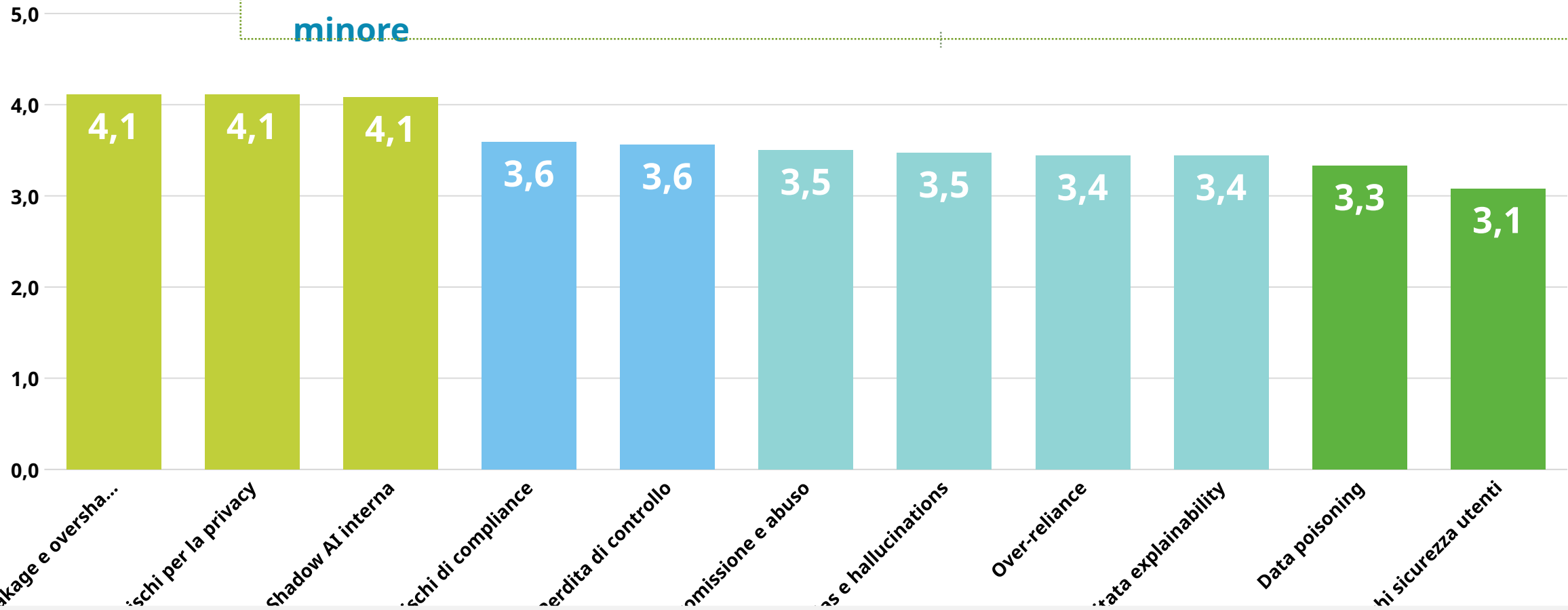
Circa il **10%** delle organizzazioni ha **integrato** i **rischi** specifici per la **GenAI** nei propri framework di **Risk Management**.



Percezione e gestione del rischio AI

Severity dei rischi GenAI secondo i CISO

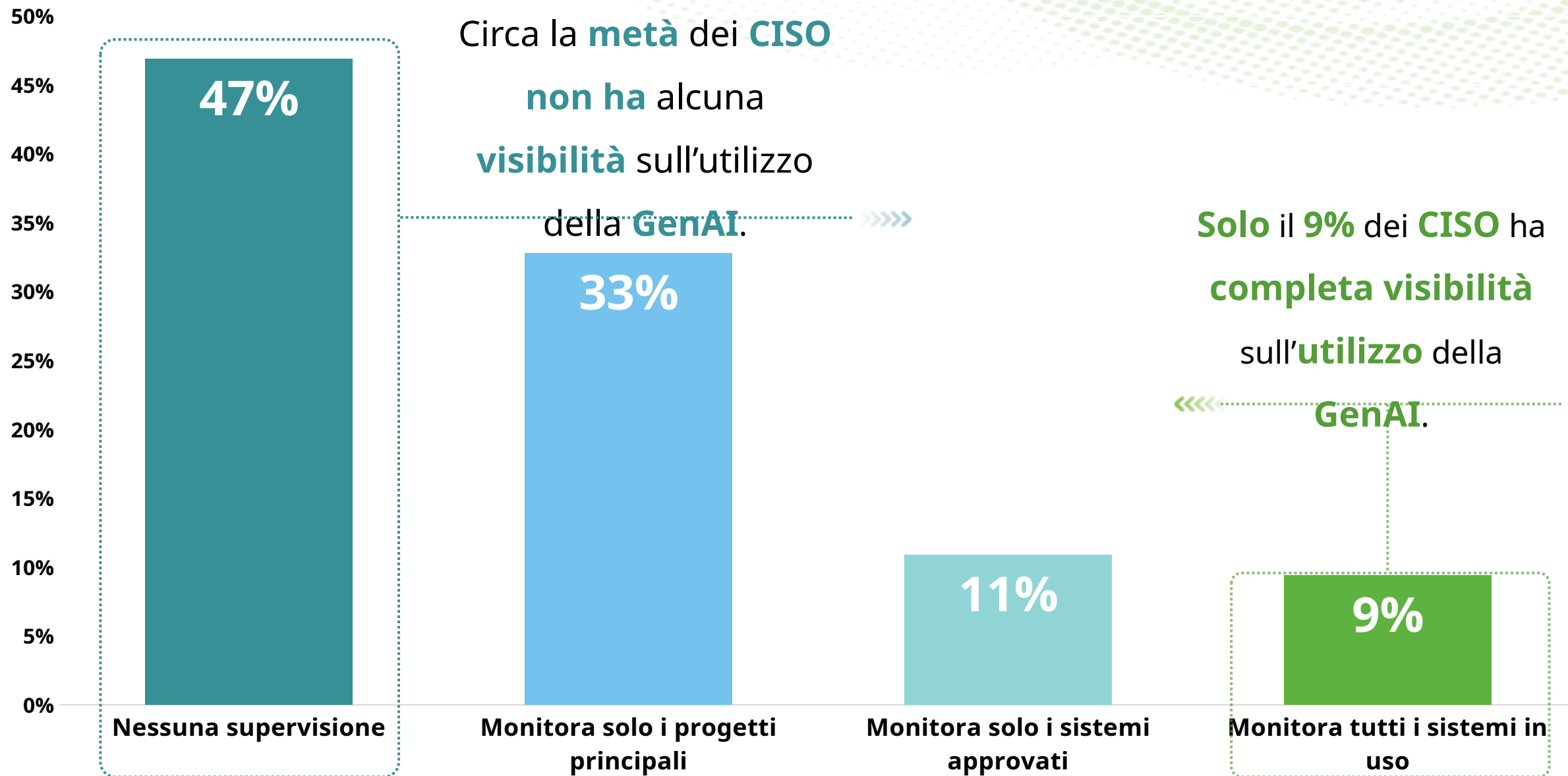
- I **rischi AI** percepiti come più **critici** restano quelli **tradizionali**
- Le **minacce** specifiche per l'**AI** e per gli **agenti** sono ancora considerate a **severity minore**



Legenda: La severity dei rischi GenAI è calcolata su una scala da 0 (rischio trascurabile) a 5 (rischio critico).

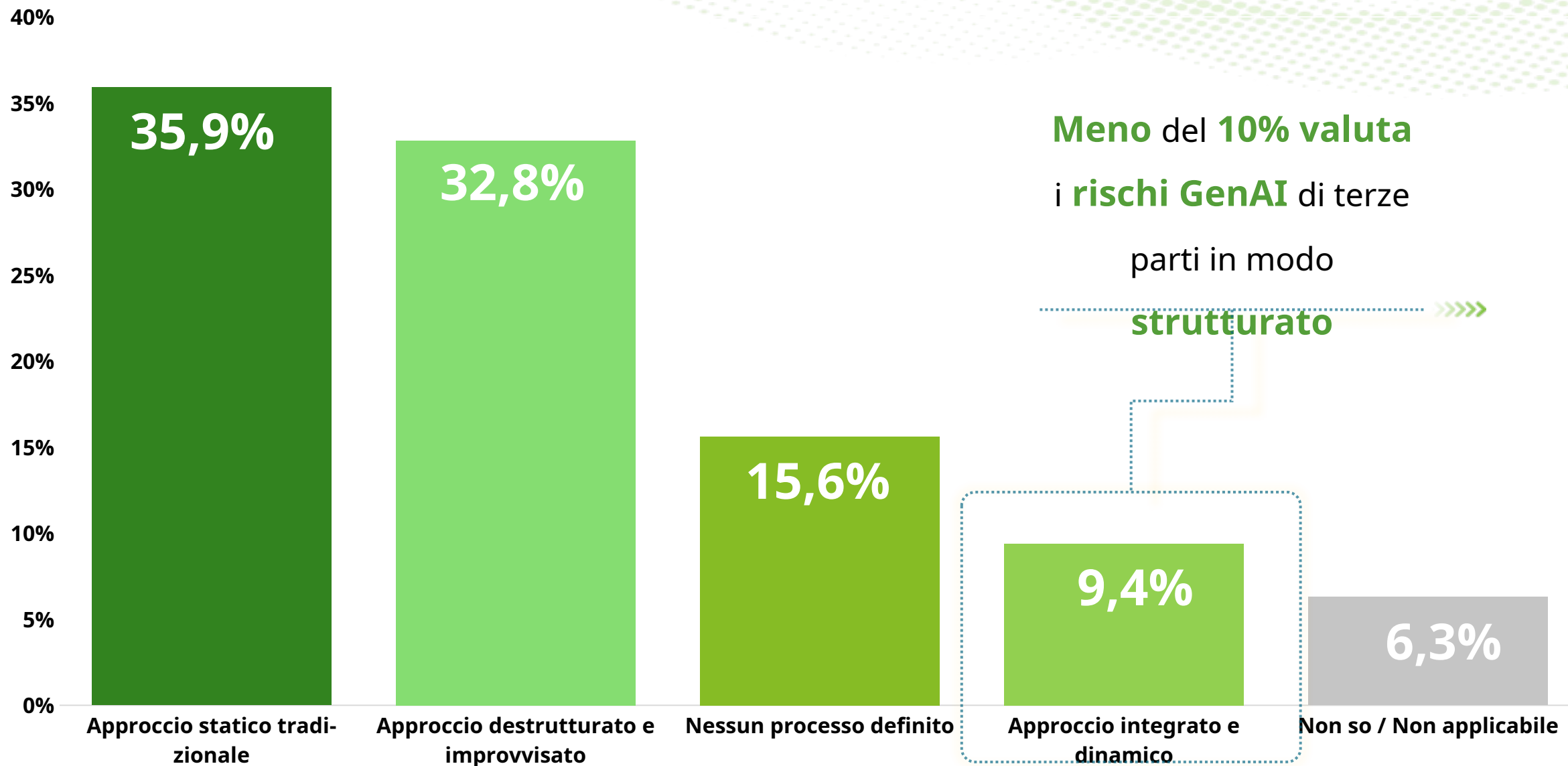
Percezione e gestione del rischio AI

Visibilità dei CISO sull'uso della GenAI



Percezione e gestione del rischio AI

Approcci di valutazione del rischio per prodotti AI



Percezione e gestione del rischio AI

Il gap fra i rischi identificati e la strategia di sicurezza

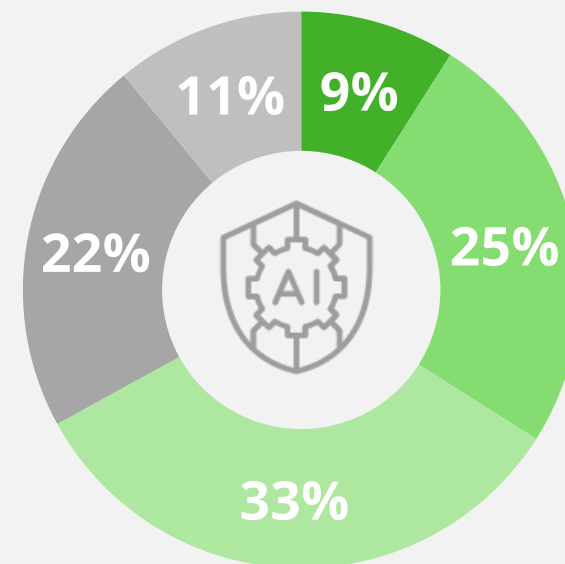


I **CISO** riconoscono i **rischi** della **GenAI**, ma **non** hanno una **strategia** di **sicurezza** **matura**.

Solo il **9%** ha una **strategia** di **sicurezza** **GenAI** definita e implementata.

L'**11 %** **non considera** la **sicurezza** **GenAI** come una **priorità**.

Stato di definizione della strategia di sicurezza AI



- Definita e implementata
- Definita ma non completamente implementata
- In fase di sviluppo (non ancora finalizzata)
- Non definita, ma pianificata
- Non definita e non prioritaria

Percezione e gestione del rischio AI

Divario tra governance e misure tecniche di enforcement

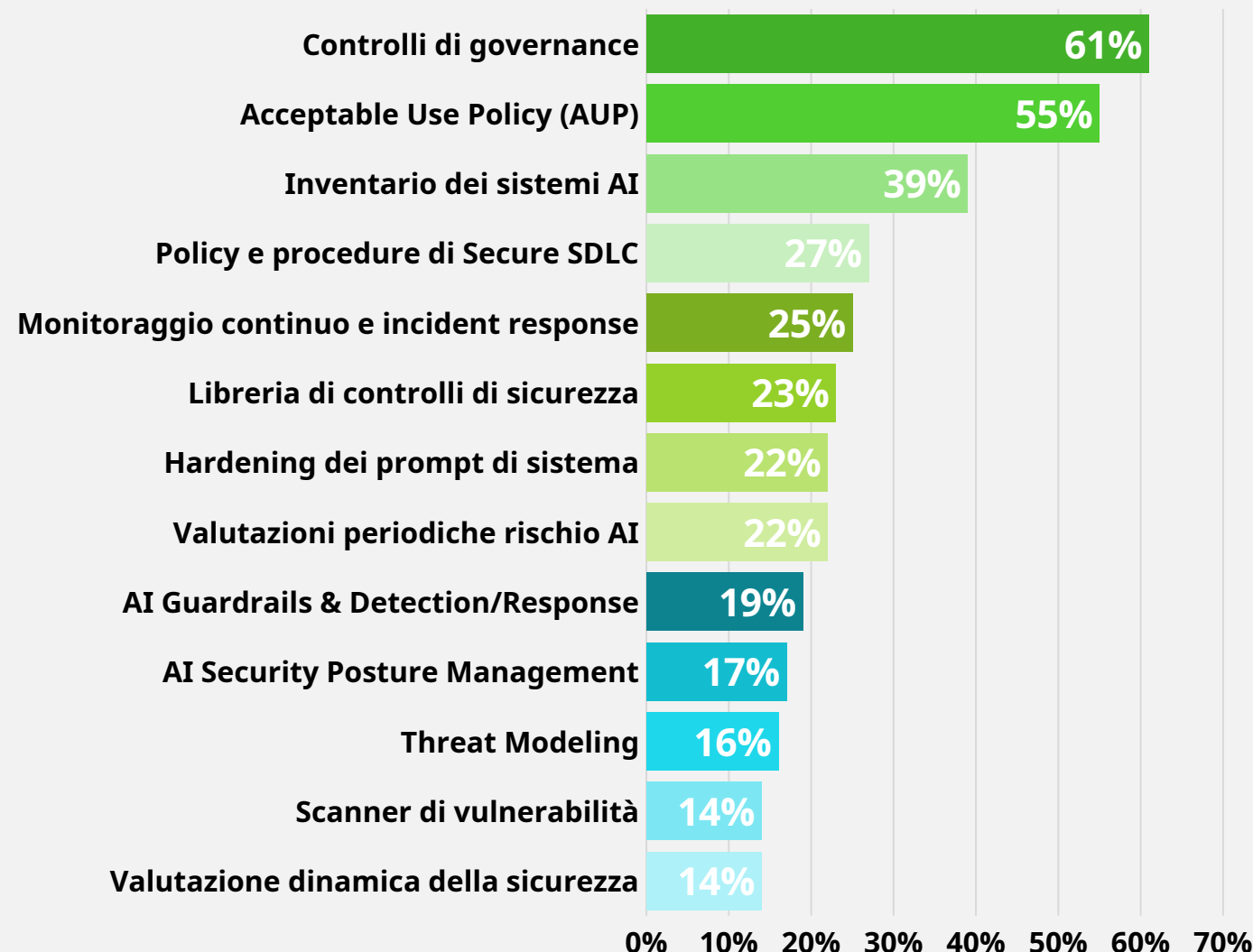


La **sicurezza** della **GenAI** è guidata da **policy** e **governance** con **controlli tecnici** ed **enforcement limitati**.

60% adotta un **approccio policy-first** alla sicurezza.

~40% dispone di un **inventario** dei **sistemi AI**.

Misure di sicurezza implementate



Percezione e gestione del rischio AI

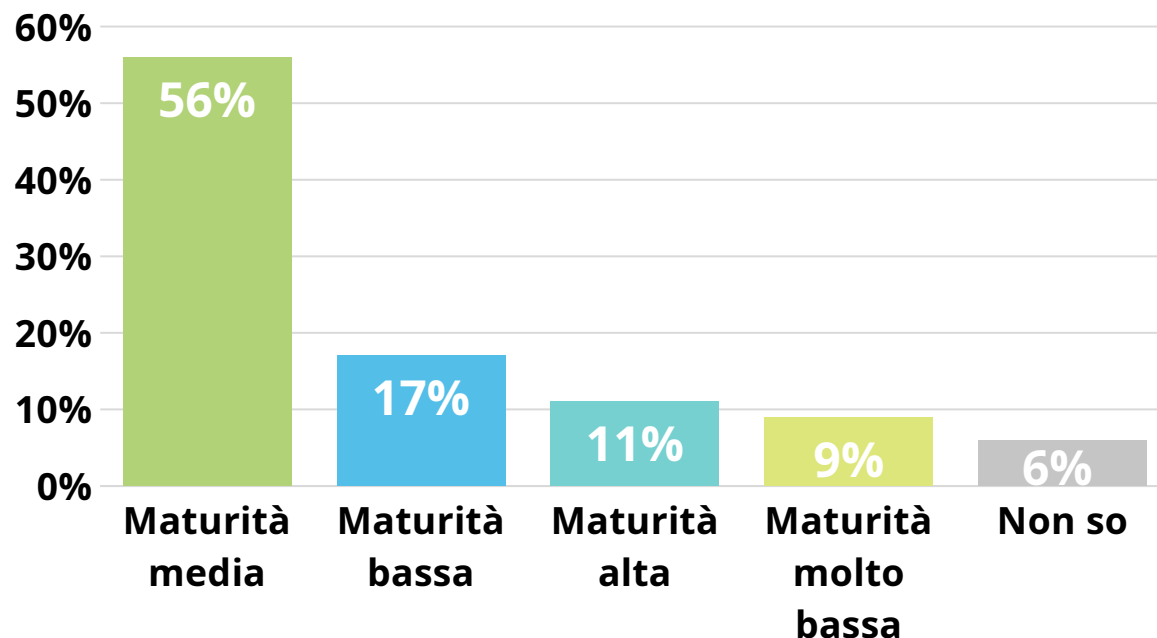
Stato del mercato tecnologico in ambito AI Security



67%

dei **CISO** considera il **mercato tecnologico** a un **livello** di **maturità medio-alta...**

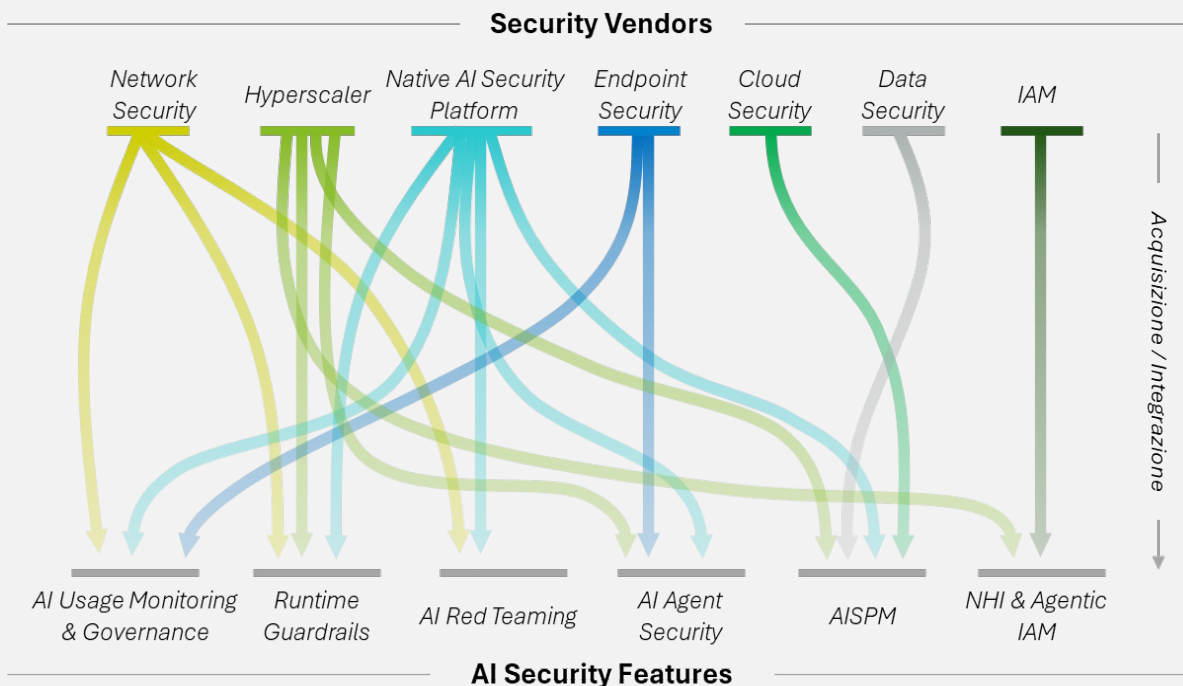
Percezione maturità tecnologie sicurezza GenAI



... ma i Key Market Trends rilevano

- La “**feature collision**” erode i **confini** tra **categorie**
- Molte **capability** saranno integrate **by default** nello **stack** già **in uso**
- **Estendere le capability** o **consolidarle**?

Valutazione del rischio degli strumenti GenAI



Cluster di maturità e roadmap per i CISO

I cinque cluster di maturità per l'AI Security

32% *Beginners*

Assenza di strategia e gestione della sicurezza AI non strutturata.

Maturità



22% *Planners*

Governance e strategia chiare, ma execution non ancora coerente.



10% *Executors*

Solide misure operative ma senza un framework di governance solido.



33% *Practitioners*

Postura in costruzione con approccio bilanciato e maturità moderata.



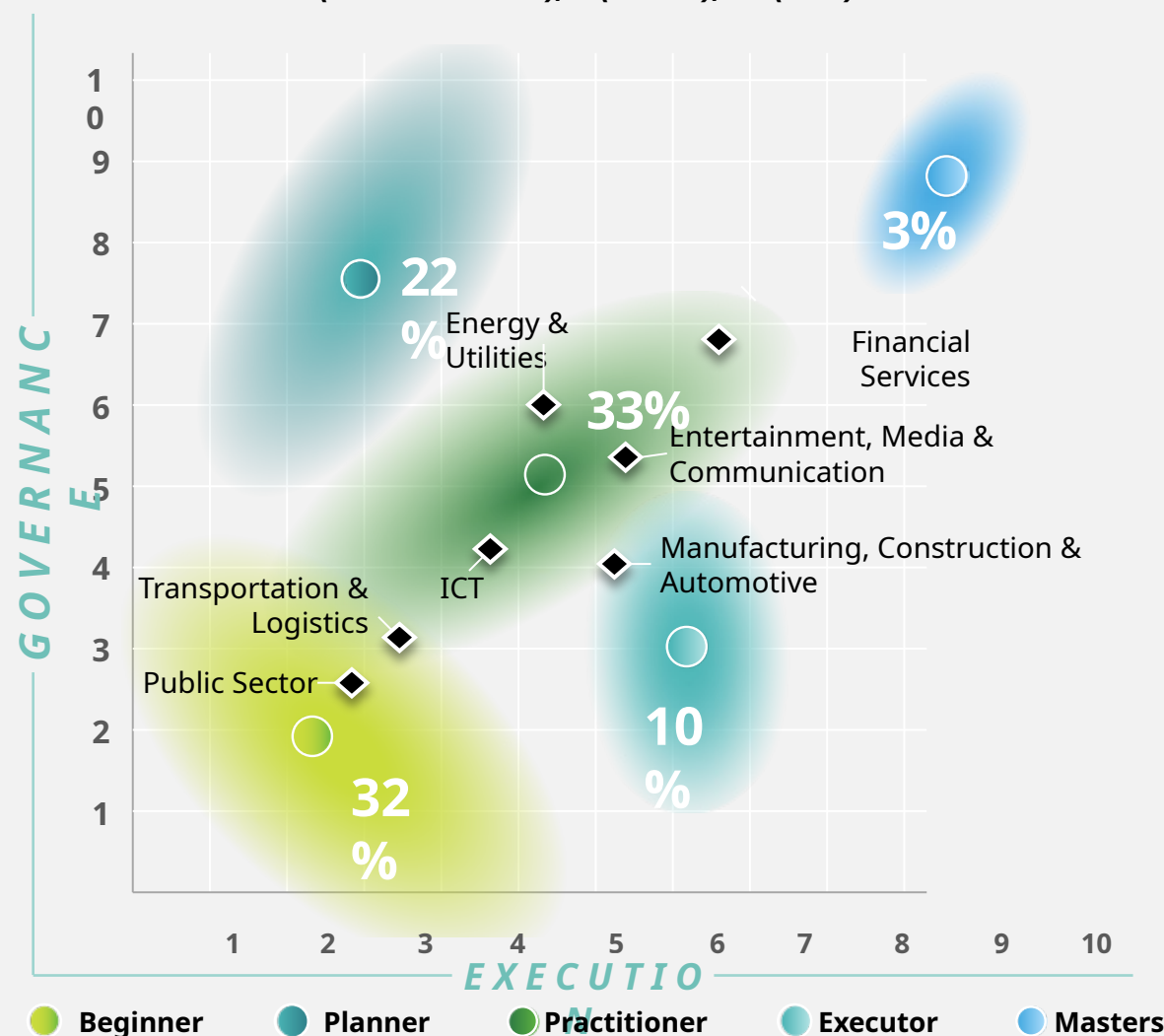
3% *Masters*

Governance robusta e misure tecniche avanzate pienamente allineate.



Maturità media dei principali settori economici

Scala Maturità: 0-1 (Assente/Bassa), 5 (Media), 10 (Alta).



Cluster di maturità e roadmap per i CISO

Il modello di maturità progressivo dell'AI Security



Una **postura** di **sicurezza adeguata** si costruisce attraverso un **percorso evolutivo** verso una **governance** solida e un'**execution** strutturata.



1

Foundation

- AI Governance & Steering Committee
- Strategia di AI Security
- Allocazione Budget



2

Structuring

- AI Risk
- AI Security Frameworks
- Processi & Procedure di Security



3

Operationalization

- Tecnologie di AI Security
- AI Security by Design & Testing
- Programmi di AI Risk Awareness



4

Optimization

- Assessment & Measurement
- Continuous Improvement
- Innovation Scouting

Cluster di maturità e roadmap per i CISO

Wrap-up



La **maturità complessiva** è ancora **limitata**. L'**AI Security** **non** è un **problema** del **domani ma** dell'**oggi**.



Governance senza execution è solo compliance, mentre execution senza governance è caos. È **necessaria** una **strategia bilanciata** e **allineata** agli **obiettivi** di **business**.



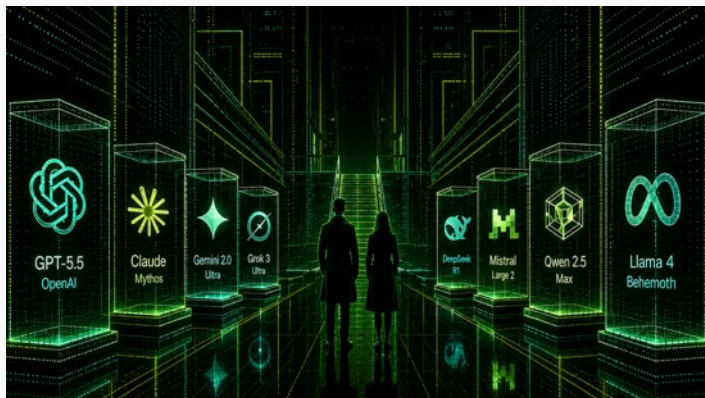
Il **CISO** deve passare da **gestore** del **rischio residuo** a **co-architetto** della **trasformazione AI**.



Prospettive future sulla sicurezza dell'AI

Dimensioni evolutive dell'AI

Evoluzione del Threat Landscape



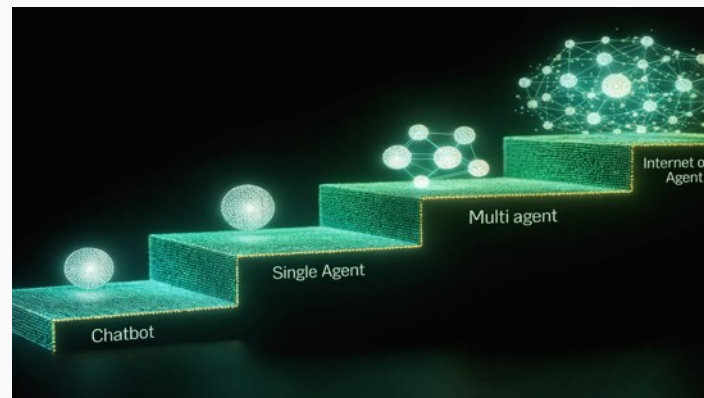
L'impatto della **Frontier AI** dalla
prospettiva di un **CISO**

Urgenza per i CISO

IMMEDIATA



Evoluzione Architeturale



L'**ascesa** dell'**Agentic AI**, dai
chatbot all'**Internet of Agents**

Urgenza per i CISO

ALTA



Evoluzione Infrastrutturale



Edge AI e il nuovo paradigma
dell'**intelligenza distribuita**

Urgenza per i CISO

PROSPETTICA



Cyber Resilience Acceleration Program



Deloitte.

Governance & Risk Management

Strategy | Roadmap | DORA | NIS2 | AI Act
| Compliance | Organizational Readiness



AI-Powered Prevention

AI Defense Plan | AI Network Firewall



Continuous Threat Exposure Management

Exposure Discovery | Vulnerability
Prioritization | Attack Path Analysis

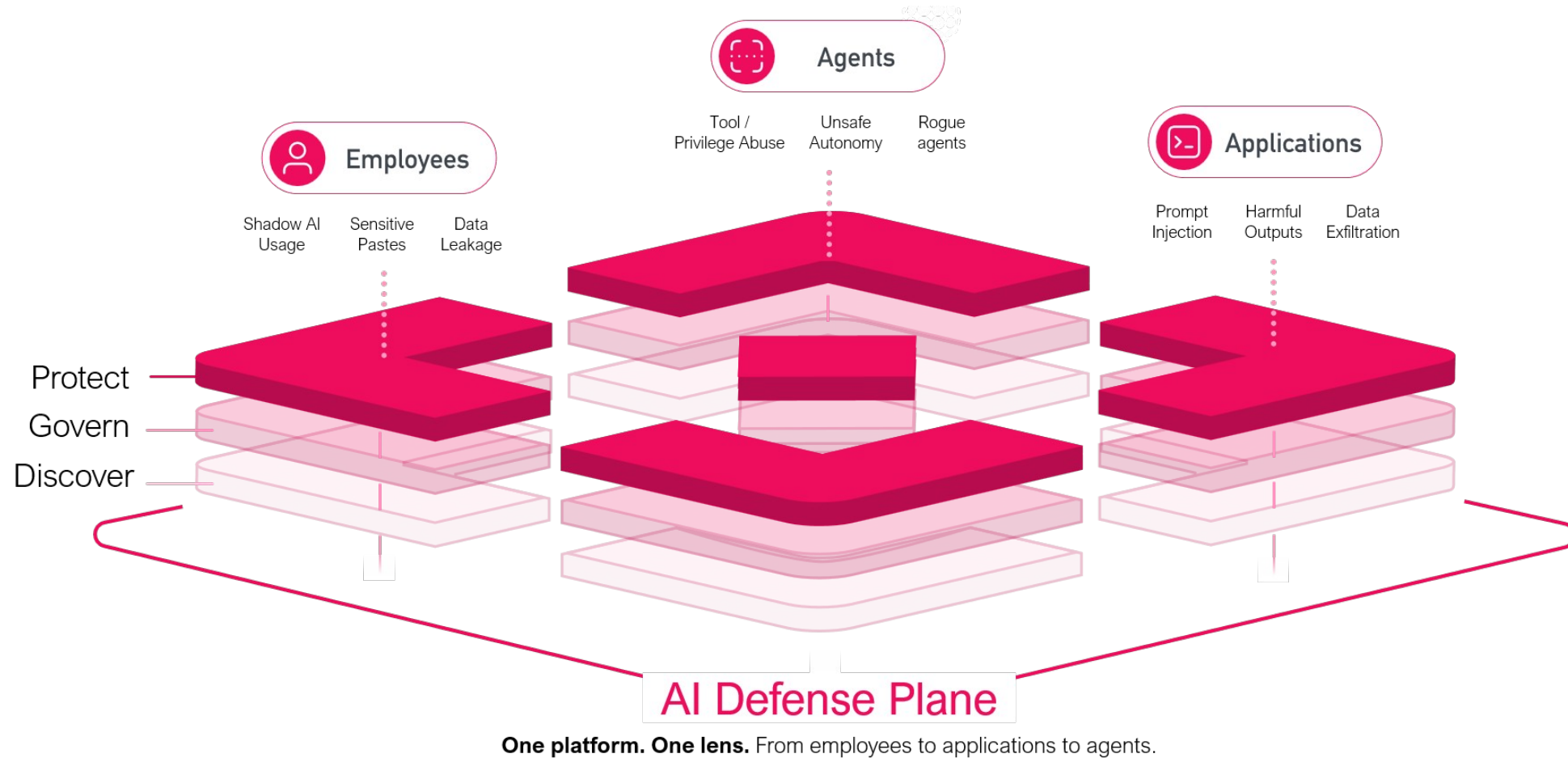


Breach Containment

Microsegmentation | Zero Trust
Segmentation | Ransomware Containment
| Lateral Movement Prevention



Check Point Framework - AI Defense Plane



Check Point Framework - AI Defense Plane



Workforce AI Security

Discovery, governance e difesa in tempo reale per l'uso dell'IA dei dipendenti.

AI Agent Security

Visibilità e protezione in tempo reale per applicazioni e agenti di IA



AI Red Teaming

Valutazioni delle minacce basate sul rischio

Cyber Resilience Acceleration Program



Deloitte.

Governance & Risk Management

Strategy | Roadmap | DORA | NIS2 | AI Act
| Compliance | Organizational Readiness



Breach Containment

illumio

Microsegmentation | Zero Trust
Segmentation | Ransomware Containment
| Lateral Movement Prevention

CHECK POINT
SERVICES

AI-Powered Prevention

AI Defense Plan | AI Network Firewall



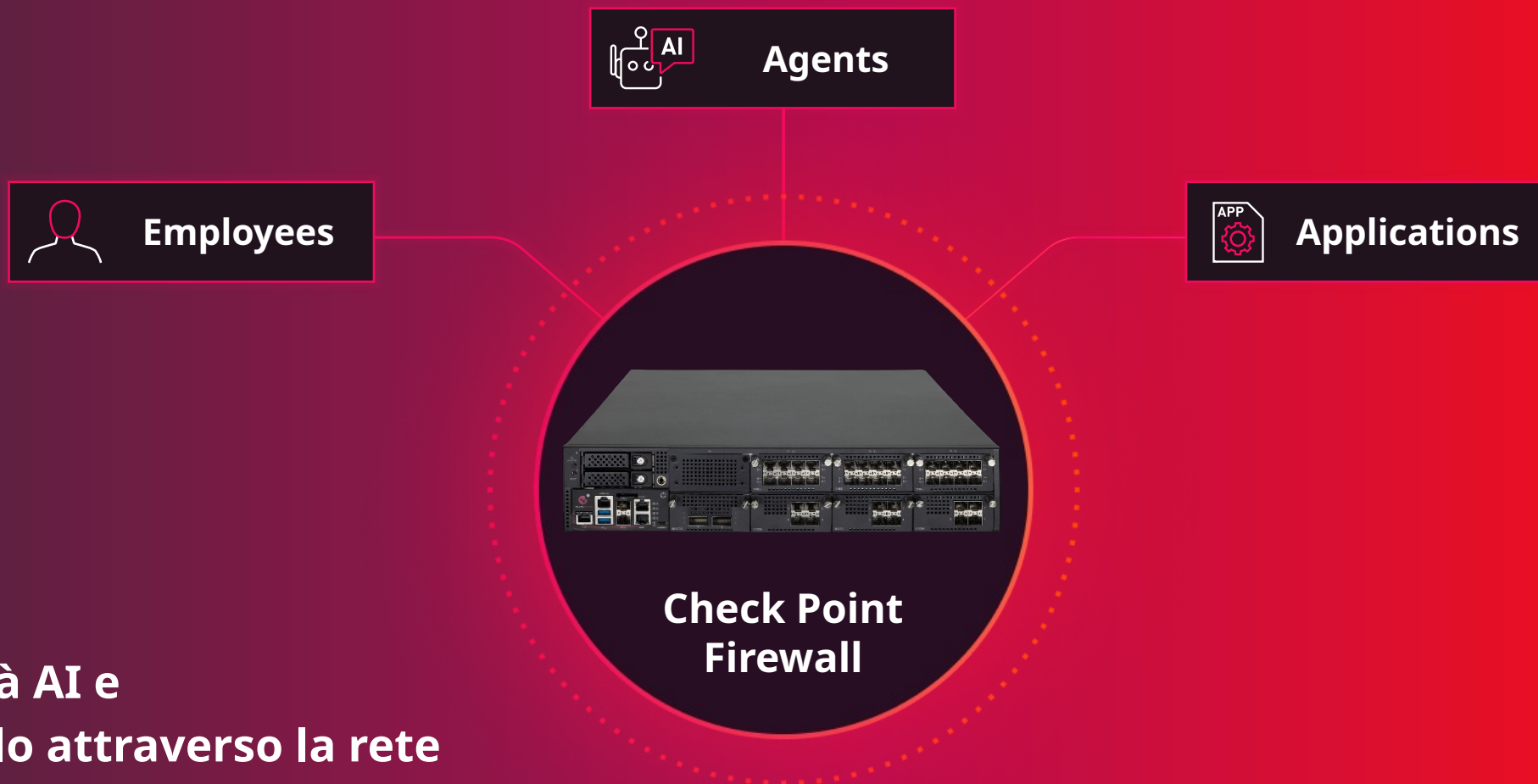
CHECK POINT
SERVICES

Continuous Threat Exposure Management

Exposure Discovery | Vulnerability
Prioritization | Attack Path Analysis



AI Network Firewall



Visibilità AI e
Controllo attraverso la rete

AI Network Firewall



Employees



Check Point
Firewall

Visibilità AI e
Controllo attraverso la rete

Scopri App, Strumenti di IA e attività Shadow AI. Acquisisci visibilità su prompt e obiettivi

*Governare con Controlli di Accesso e Sicurezza.
Gestire l'accesso alle applicazioni di IA*

*Proteggere i dati sensibili
Prevenire la perdita di dati*

AI Network Firewall



 **Agents**



**Check Point
Firewall**

Governare lo scopo e le azioni dell'agente

Limitare l'uso degli strumenti dinamicamente in base al contesto e al rischio

Far rispettare automaticamente la sicurezza durante l'esecuzione

**Visibilità AI e
Controllo attraverso la rete**

AI Network Firewall



Prevenire prompt injection e inputs malevoli

Ferma la manipolazione dei modelli prima che abbia un impatto sull'azienda

Guardrail per proteggere i modelli di IA locali e distribuiti



**Check Point
Firewall**



Applications

Cyber Resilience Acceleration Program



Deloitte

Governance & Risk Management

Strategy | Roadmap | DORA | NIS2 | AI Act
| Compliance | Organizational Readiness



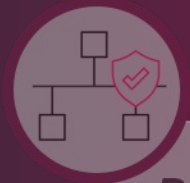
AI-Powered Prevention

AI Defense Plan | AI Network Firewall



Continuous Threat Exposure Management

Exposure Discovery | Vulnerability
Prioritization | Attack Path Analysis



illumio

Breach Containment

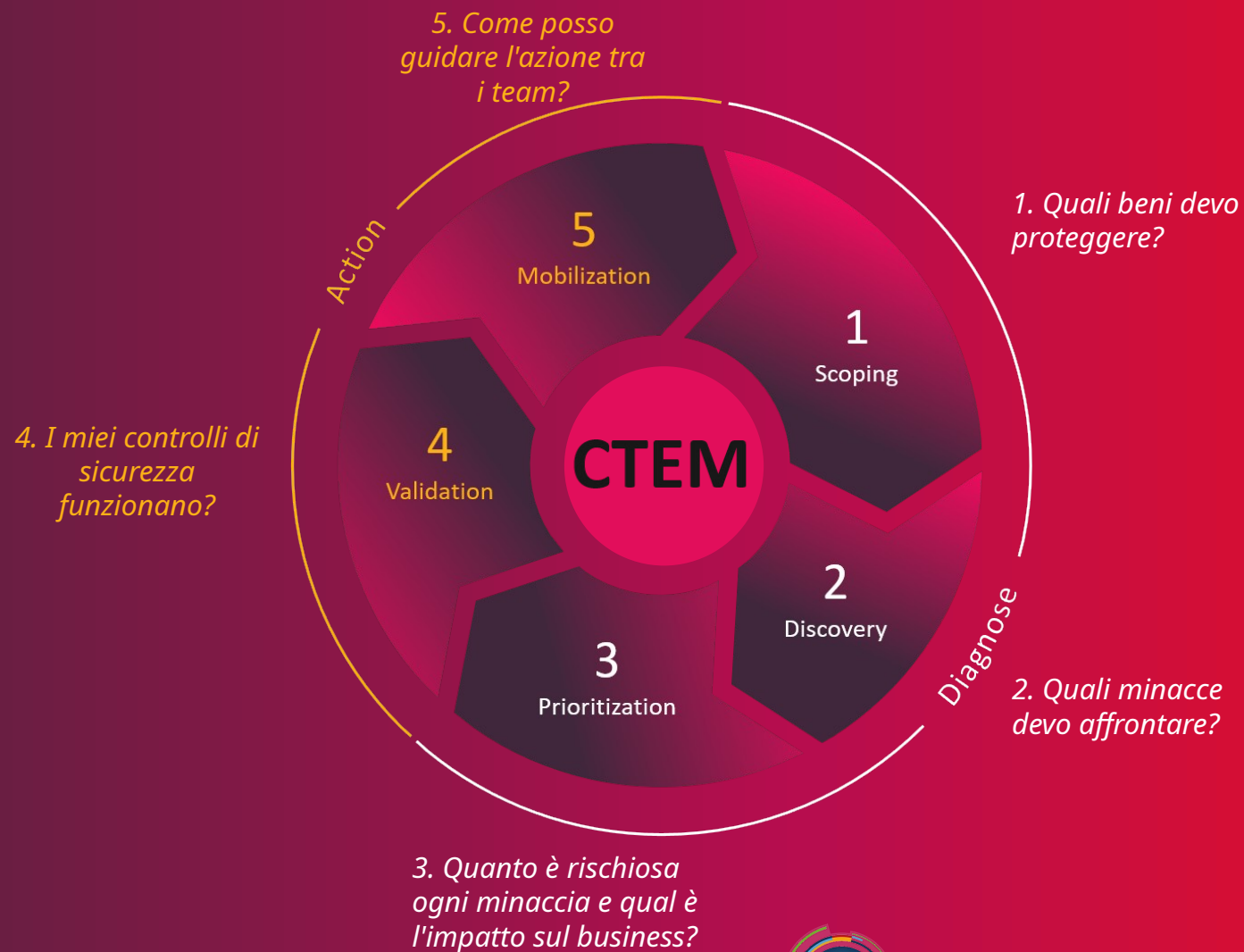
Microsegmentation | Zero Trust
Segmentation | Ransomware Containment
| Lateral Movement Prevention



Continuous Threat Exposure Management (CTEM)



Un framework creato da Gartner per affrontare l'esposizione e in ambienti complessi e multi-team



Intelligence-led, Remediation-driven



Safe Remediation

Puoi fidarti della bonifica applicata:
controlli di sicurezza per patchare
Diffusione e massimizzazione dell'intelligenza

- Blocco dell'infrastruttura degli attaccanti

Exposure Prioritization

Prioritizzazione che riflette il rischio reale
Configurazioni errate di asset interni ed esterni
Deduplicazioni e falsi positivi

- Vulnerabilità non patchate: rete, OS e app

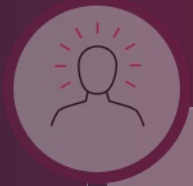


Threat Intelligence

Informazioni che mostrano cosa viene usato come arma:
Strumenti e infrastrutture usate dagli attaccanti
Informazioni dal Dark Web e campagne attive

- Segnali di Brand Impersonation

Cyber Resilience Acceleration Program



Deloitte

Governance & Risk Management

Strategy | Roadmap | DORA | NIS2 | AI Act
| Compliance | Organizational Readiness



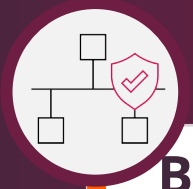
AI-Powered Prevention

AI Defense Plan | AI Network Firewall



Continuous Threat Exposure Management

Exposure Discovery | Vulnerability
Prioritization | Attack Path Analysis



Breach Containment illumio

Microsegmentation | Zero Trust
Segmentation | Ransomware
Containment | Lateral Movement
Prevention



Resilienza Operativa nell'Era dell'AI

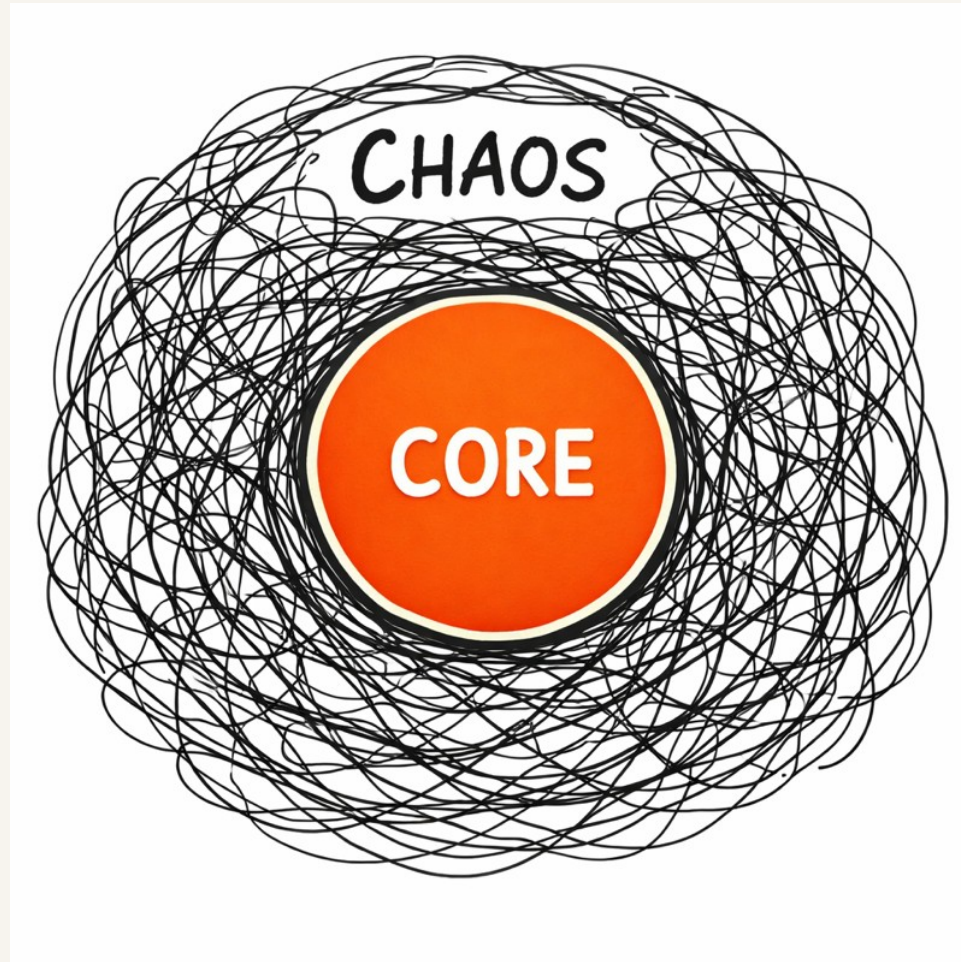
Le recenti evoluzioni dell'AI, evidenziate anche dal caso Mythos, stanno accelerando la capacità di individuare e sfruttare vulnerabilità su larga scala, rendendo ancora più centrale il tema della resilienza operativa.

Sep. 2026



Proteggere il Core, non Controllare il Caos

- L'AI accelera il rischio.
- La compromissione è una possibilità.
- La continuità operativa è un requisito.



Non possiamo garantire l'assenza di incidenti. Possiamo garantirne il contenimento.

**// La prevenzione riduce la
probabilità.
La resilienza riduce
l'impatto.**



Garantire la continuità dei servizi essenziali in un contesto di rischio sempre più complesso.

The Broken Math

Prevention & patching can't carry the load

1

Patch backlog permanenti

Dipendenze, finestre di test e change management rendono inevitabili backlog anche nelle organizzazioni più mature.

2

Tempi di remediation incompatibili con il rischio

Le minacce evolvono più rapidamente dei cicli tradizionali di patching e aggiornamento.

3

La prevenzione non può essere l'unica strategia

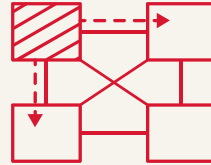
Ridurre la probabilità è fondamentale. Garantire la continuità operativa è essenziale.

Perché gli attacchi hanno successo?



La prevenzione e il rilevamento falliscono

- Nessun controllo ha efficacia del 100%
- Gli attaccanti mantengono l'accesso per settimane o mesi



L'attacco si propaga

- Il movimento laterale consente di raggiungere sistemi critici
- Ambienti complessi e interconnessi amplificano il rischio

In un mondo ibrido, multi-cloud e altamente interconnesso, il movimento laterale è il principale fattore di amplificazione del rischio.



I servizi critici vengono impattati

- Interruzione di applicazioni e processi essenziali
- Rischi operativi, normativi e reputazionali

//

La BCE indica segmentazione, microsegmentazione e Zero Trust come misure a supporto della defence-in-depth.

Segmentation and, where feasible, micro-segmentation, together with the adoption of zero-trust principles [...] can support defence-in-depth.

ECB Supervisory Board Letter SSM-2026-0301
Annex 1, point 5 | 7 July 2026

Non conta solo prevenire.
Conta continuare a operare.

Fonte: ECB, "Addressing AI-enabled cybersecurity threats"



Le organizzazioni devono dare priorità alla resilienza e al contenimento

44%

non è in grado di identificare e contenere rapidamente un attacco

35%

segnala una mancanza di visibilità negli ambienti ibridi che rende più difficile rispondere agli attacchi

55%

degli attacchi si propaga lateralmente verso altri sistemi

Perchè Illumio?

Ridurre l'impatto di un attacco quando la prevenzione non è sufficiente

1

Continuous real-time observability

Comprendere le comunicazioni e le dipendenze tra applicazioni, workload e servizi.

2

Segmentazione e Contenimento

Limitare il movimento laterale prima che raggiunga sistemi critici.

3

Riduzione del Blast Radius

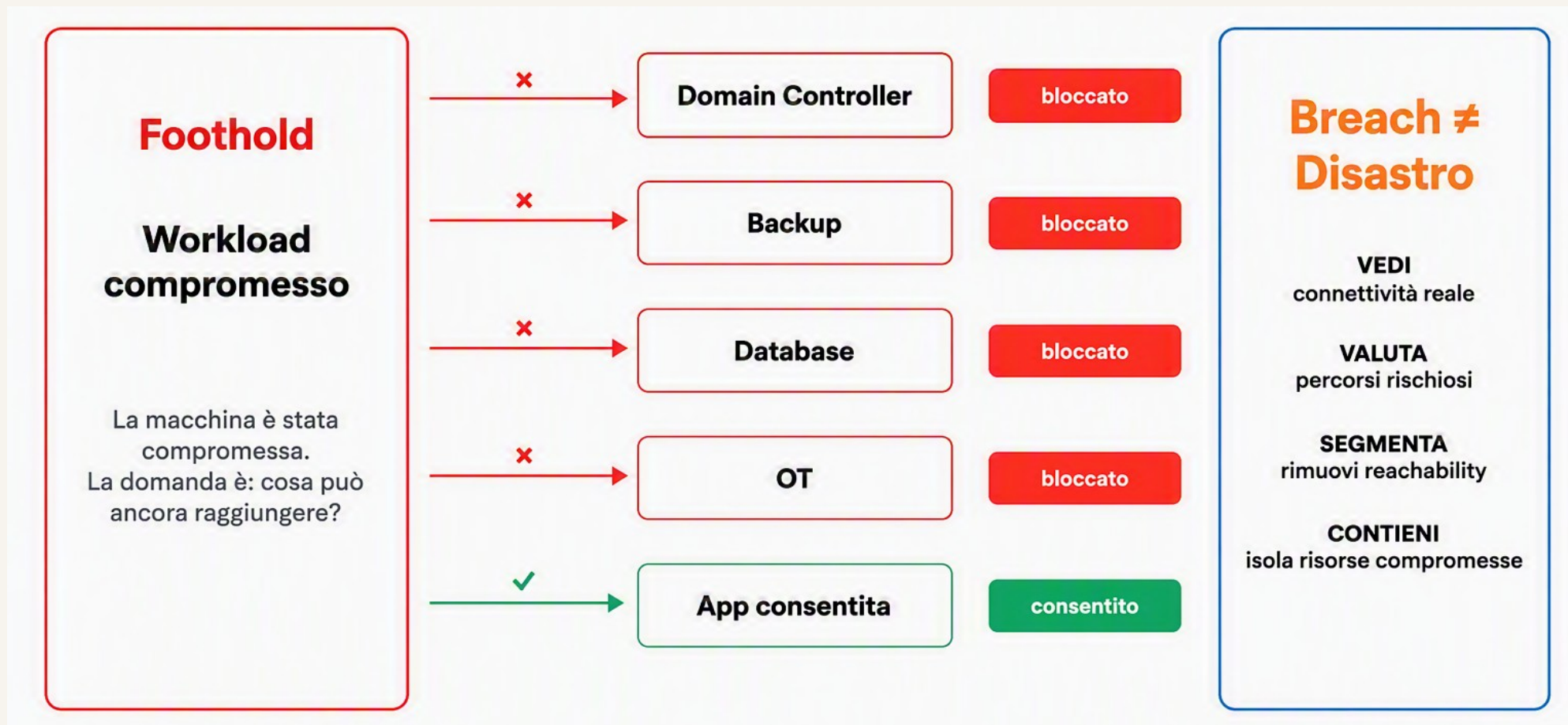
Trasformare un potenziale incidente sistemico in un evento circoscritto.

4

Resilienza Operativa

Proteggere la continuità dei servizi essenziali anche durante un attacco.

Il breach resta un incidente. La propagazione non è data per scontata.



// Breach containment is non-negotiable in the age of AI.
AI makes compromise cheaper, faster, and more scalable.
Containment makes it survivable.



Question & Answer



Deloitte.

Governance & Risk Management

Strategy | Roadmap | DORA | NIS2 | AI Act
| Compliance | Organizational Readiness



illumio

Breach Containment

Microsegmentation | Zero Trust
Segmentation | Ransomware Containment
| Lateral Movement Prevention

CHECK POINT
SERVICES



AI-Powered Prevention

AI Defense Plan | AI Network Firewall

CHECK POINT
SERVICES



Continuous Threat Exposure Management

Exposure Discovery | Vulnerability
Prioritization | Attack Path Analysis

