GOBEYOND 2026

WHERE TECH ACCELERATES BUSINESS

IT ECOSYSTEM · CYBERSECURITY · DIGITAL IDENTITY

24 Marzo 2026 | Hotel NHOW Milano

Centralizzazione e AI nella sicurezza informatica

un modello per la gestione delle identità digitali

Vincenzo Calabrò

Funzionario alla Sicurezza CIS Ministero dell'Interno
Professore a contratto in Tecnologie per la Sicurezza Informatica

Evento di IKN ITALY YOUR KNOWLEDGE NETWORK

Analisi del contesto: gli asset digitali di un'organizzazione

- **Eterogeneità - Promiscuità**
  - Assets on-premise
  - Assets in cloud
  - Utenti in smart-working
  - Mobile device – Dispositivi BYOD
- **Complessità**
  - Applicazioni Cloud native vs Legacy
  - Comunicazioni tramite API vs Plain text
  - Tecnologie innovative: SaaS, IoT, AI
- **Maggiore Esposizione**
  - Threat actors
  - Minacce
  - Vulnerabilità

Zero Trust: il nuovo paradigma per governare la security in rete

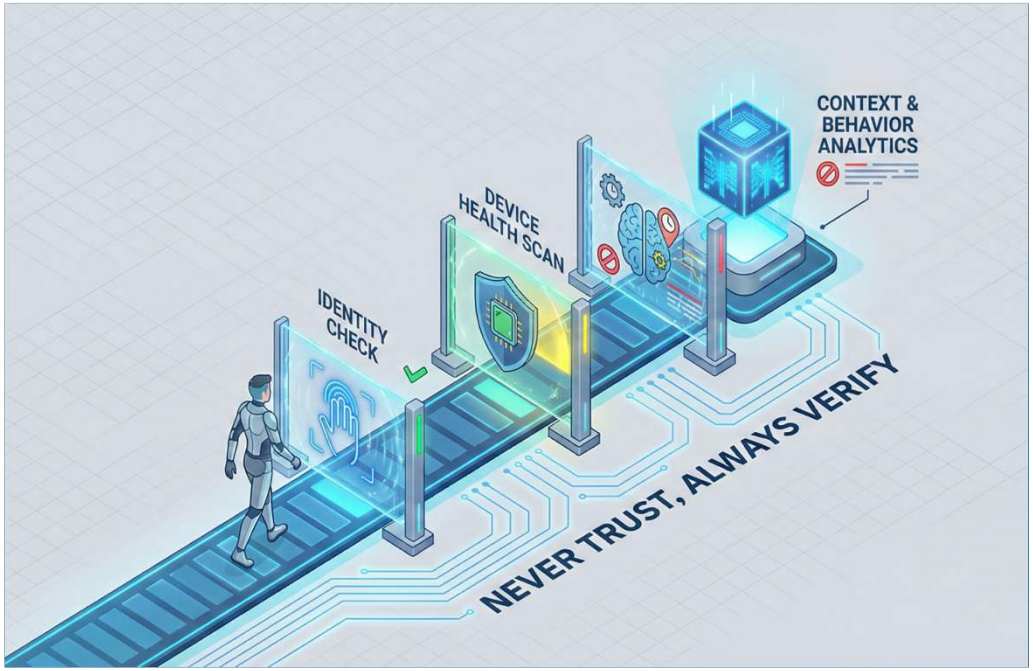
La teoria dello "**Zero Trust**", che si basa sul principio fondamentale "**non fidarsi mai, verificare sempre**", si fonda su questi principi cardine:

- **Micro-segmentazione**: non esiste un "dentro" sicuro. Tutto è diviso in piccole isole protette.
- **Privilegio minimo**: accesso limitato alle sole risorse necessarie per svolgere la specifica mansione, riducendo l'impatto di una potenziale violazione.
- **Verifica esplicita e continua**: l'accesso non è una porta singola, ma una serie infinita di checkpoint.
- **Identità come nuovo perimetro**: non importa dove sei, importa chi sei e lo stato del tuo dispositivo in quel momento.

Sicurezza costruita sull’Identità

Nel contesto attuale, non è più sufficiente concentrarsi sulla sicurezza perimetrale, ma è necessario implementare un sistema che consenta all'organizzazione di:

- **Gestire** il ciclo di vita delle identità digitali (umane, agenti, oggetti digitali)
- **Diversificare** i metodi di autenticazione per adattarli alla criticità dell’asset
- **Integrare** i vari modelli tecnologici (LDAP, Radius, SSO, Wallet/SSI)
- **Concedere** le autorizzazioni adeguate
- **Monitorare** gli accessi e i comportamenti degli utenti



Identity & Access Management: la soluzione

La gestione delle identità digitali rappresenta attualmente una delle sfide più complesse per le organizzazioni.

Con l'aumento esponenziale dei sistemi, delle applicazioni, delle interfacce e dei dispositivi connessi, la necessità di un approccio centralizzato rende la gestione delle identità digitali **più sicura, resiliente, scalabile e proattiva**.

Sicurezza Rinforzata

La riduzione delle superfici di attacco e la standardizzazione delle politiche di sicurezza sono tra gli obiettivi primari di un punto unico di controllo.

Efficienza Operativa

L'implementazione di un sistema di gestione delle identità consente una riduzione dei tempi associati alle procedure di provisioning e de-provisioning.

Conformità Garantita

L'allineamento con le normative della NIS 2, GDPR, con la norma ISO 27001 e con gli standard del settore è garantito da audit centralizzati.

NIST Cybersecurity Framework

L'implementazione dell'Identity and Access Management non garantisce la risoluzione dei problemi di sicurezza.

Il framework NIST (National Institute of Standards and Technology) fornisce una struttura organica per la gestione e la riduzione dei rischi di cyber-sicurezza.

- nella fase di **IDENTIFICATION**, il framework cataloga gli asset e le vulnerabilità associate
- nella fase di **PROTECTION** definisce gli standard, le politiche e i controlli da implementare preventivamente
- nella fase di **DETECTION** rileva gli eventi avversi o anomali
- nella fase di **RESPOND** attiva le misure di mitigazioni

"Al fine di garantire un funzionamento ottimale, è necessario che il framework sia alimentato da informazioni in tempo reale. In tale contesto, si rende imprescindibile l'implementazione di un sistema di gestione delle identità e degli accessi centralizzato."

Artificial Intelligence: rilevamento anomalo e gestione intelligente

L'impiego dell'intelligenza artificiale per l'analisi dei comportamenti anomali e l'ottimizzazione della gestione delle identità risulta fondamentale per migliorare la sicurezza complessiva.

Analisi Comportamentale

L'intelligenza artificiale analizza pattern di accesso, orari, dispositivi e geolocalizzazioni per creare profili comportamentali unici di ogni utente.

Rilevamento Proattivo

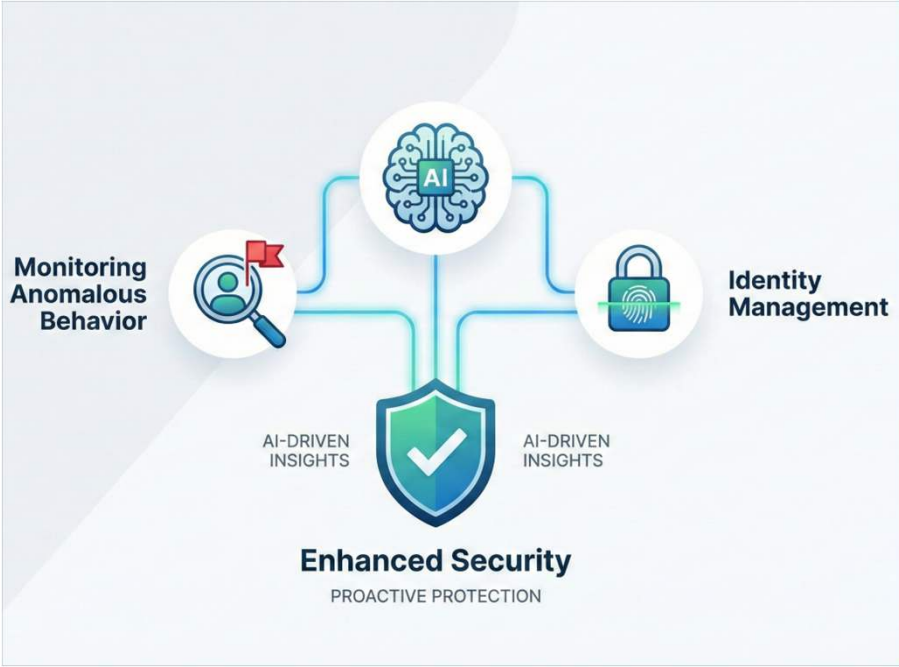
Gli algoritmi di machine learning sono in grado di identificare attività sospette in tempo reale, generando alert contestuali e riducendo i falsi positivi.

Risposta Automatica

Un sistema SOAR è in grado di implementare contromisure automatiche quali il blocco degli accessi, la revoca dei privilegi e l'isolamento dei sistemi.

Autenticazione Adattiva

Il sistema di autenticazione intelligente (IAS) prevede la modulazione del livello di sicurezza in base al rischio calcolato, richiedendo l'impiego di metodi multipli solo quando necessario.



Implementazione: percorso consigliato

PRIMA: Sistemi distinti	DURANTE: Consolidamento	DOPO: Sistema ottimizzato
Stato iniziale: Sistemi di autenticazione isolati, politiche non uniformi, interventi manuali frequenti	**Struttura comune**: Piattaforma IAM unificata, protocolli standard SAML/OAuth	**Gestione centralizzata**: Identità unificate con controllo privilegi e audit automatizzato
Strumenti isolati: LDAP, Active Directory, database proprietari non integrati	**Deployment IA**: Sistemi UEBA per analisi comportamenti, SIEM per correlazione eventi	**Difesa attiva**: Threat detection predittivo, risposta automatica agli incidenti, audit conformità semplificati
Rilevamento: Log manuali, corrispondenza via email, risposta lenta agli incidenti	**Staff tecnico**: Formazione su NIST, incident response team, procedures definite	**Operazioni snelle**: Onboarding/revoca ad automatizzazione completa, helpdesk ridotto


GOBEYOND 2026
WHERE TECH ACCELERATES BUSINESS
IT ECOSYSTEM
CYBERSECURITY
DIGITAL IDENTITY
GRAZIE!
Evento di
IKN ITALY
YOUR KNOWLEDGE NETWORK