Insight

Identity Security: guida strategica per gli acquisti

Indice

Identity Security: guida strategica per gli acquisti

Nelle aziende moderne, ogni login utente, account di servizio e connessione di terze parti rappresenta un potenziale rischio. Con il lavoro ibrido, le applicazioni cloud e l'AI che stanno trasformando l'impresa, gli attaccanti puntano sempre più alle identità – non ai firewall. Dal punto di vista di un attaccante, perché forzare un accesso quando puoi rubare un'identità e accedere direttamente? Proteggere le identità digitali è diventato uno dei modi più efficaci per prevenire violazioni, controllare gli accessi e mantenere la fiducia.

Infatti, l'identità è diventata il principale vettore di attacco per le aziende:

il 93% delle organizzazioni ha subito almeno due attacchi legati alle identità nell'ultimo anno *

Per i responsabili della sicurezza, questo significa che proteggere le identità è ora una missione critica.Questa guida chiarisce i concetti chiave di Identity Security – IAM, IGA, PAM, ITDR, autenticazione multifattore, ecc. – e spiega perché ciascuno è importante per la tua organizzazione. Inoltre, evidenzia come Insight, in qualità di fornitore leader di soluzioni con solide partnership con Microsoft, possa aiutarti a costruire un programma completo di Identity Security.

*https://investors.cyberark.com/news/news-details/2024/Report-93-Of-Organizations-Had-Two-or-More-Identity-Related-Breaches-in-the-Past-Year/)

Perché la Identity security è importante

Le aziende moderne si trovano ad affrontare un'esplosione di identità digitali – dai dipendenti e clienti ai bot software e ai servizi cloud. Ogni identità rappresenta un potenziale punto di ingresso per gli attaccanti, soprattutto mentre il lavoro ibrido e l'adozione del cloud dissolvono il tradizionale perimetro di rete. Tecniche come l'ingegneria sociale e il furto di credenziali prendono di mira non solo gli utenti, ma anche gli account macchina e le identità delle applicazioni. Credenziali deboli o rubate sono un fattore nella maggior parte delle violazioni.

si stima che l'**86%** delle violazioni coinvolga credenziali rubate. sottolineando l'urgenza di solide misure di protezione delle identità.**

Oltre alla minaccia immediata delle violazioni, pratiche di gestione delle identità inadeguate comportano rischi aziendali: accesso non autorizzato a dati sensibili, mancata conformità alle normative, interruzioni operative e perdita di fiducia da parte dei clienti. Al contrario, un programma robusto di Identity Security consente di applicare i principi di "zero trust" ("mai fidarsi, verificare sempre"), garantendo che solo le persone (o i sistemi) giusti ottengano l'accesso corretto, alle condizioni appropriate. Inoltre, migliora l'esperienza utente sostituendo il caos (login multipli, processi manuali di accesso) con un accesso sicuro e semplificato – permettendo la produttività senza sacrificare la sicurezza. In sintesi, concentrarsi su Identity Security aiuta le organizzazioni a ridurre i rischi, rispettare i requisiti di conformità e potenziare il business con un accesso sicuro e affidabile alle risorse tecnologiche.

**https://keepnetlabs.com/blog/top-phishing-statistics-and-trends-you-must-know

Elementi chiave della Identity Security

Per proteggere l'organizzazione, la Identity Security deve coprire più domini. Non si tratta di un singolo prodotto, ma di un insieme interconnesso di funzionalità che, insieme, rispondono a domande fondamentali: chi (o cosa) può accedere a cosa, quando e come? Il diagramma qui sotto illustra l'intero panorama delle capacità di Identity Security – dalla gestione delle identità e dei privilegi al monitoraggio delle minacce.

Identity Strategy Framework di Insight

Identità & Accesso
Chi può accedere a cosa?

Fondamenti dell'Identità
- Directory services
- Federation / B2B
- Provisioning e de-provisioning
- Customer identity / B2C

Authentication
inclusa multi-fact "step up" authentication

Autorizzazione

Single sign-on

Self-service per l'utente

Identity Governance & Administration (IGA)
Dovrebbero ancora avere accesso?

Fondamenti dell'Identità
- Revisioni e certificazioni degli accessi
- Gestione della compliance
- Audit

Identity Administration
- Gestione dei workflow

Privileged Access
- Scoperta degli account
- Gestione delle credenziali
- Registrazione delle sessioni
- Gestione delle deleghe

Identity Threat Detection & Response (ITDR)
Siamo sotto attacco?

Threat Detection
- Rilevamento delle anomalie e analisi del comportamento di utenti ed entità (UEBA)

Threat Response
- Sospensione account o reset password
- Re-autorizzazione forzata / step-up

Gestione delle identità degli accessi (IAM)

La gestione delle identità e degli accessi (Identity and Access Management, IAM) è la base di una strategia di Identity Security. Si concentra sulla creazione e gestione delle identità digitali (per dipendenti, partner, clienti e persino account software) e sul controllo del loro accesso alle risorse. IAM copre la creazione delle identità utente nei sistemi di directory, il provisioning degli account alle applicazioni e i servizi di autenticazione come il single sign-on. In altre parole, "stabilisce il punto di partenza per chi o cosa dovrebbe avere accesso a cosa" all'interno dell'organizzazione.

In pratica, le soluzioni IAM (come Microsoft Entra ID, precedentemente Azure AD) consentono agli utenti di accedere in modo sicuro e semplice, applicare politiche sulle password o login senza password e gestire centralmente l'accesso a vari sistemi.

Perché è importante: una solida base IAM garantisce che solo utenti autenticati e autorizzati possano accedere alle risorse sensibili, riducendo il rischio di accessi non autorizzati. L'IAM centralizzato migliora la sicurezza e l'esperienza utente eliminando la proliferazione di password e consentendo agli utenti aziendali di ottenere l'accesso di cui hanno bisogno (ad esempio, tramite single sign-on alle app cloud). Inoltre, pone le basi per applicare politiche di sicurezza come l'autenticazione multifattore e l'accesso condizionale in tutta l'azienda. Senza un IAM efficace, le organizzazioni spesso affrontano controlli di accesso incoerenti e "silos" di identità, con conseguenti lacune di sicurezza, utenti frustrati e rilievi negli audit. In sintesi, l'IAM è cruciale sia per la produttività che per la sicurezza, fornendo la prima linea di difesa contro l'uso improprio delle identità.

Le principali funzionalità IAM includono: servizi di directory per archiviare e verificare le identità degli utenti, meccanismi di autenticazione (dalle password alla biometria e MFA), federazione per login di partner o clienti (B2B/B2C) e processi di provisioning/de-provisioning per concedere e revocare l'accesso quando le persone entrano, si spostano o lasciano l'organizzazione. L'IAM moderno enfatizza l'autenticazione forte e l'accesso basato sul contesto (approfondito più avanti), poiché gli attaccanti prendono sempre più di mira le credenziali di accesso.

Governance e amministrazione delle identità (IGA)

La governance e amministrazione delle identità (Identity Governance and Administration, IGA) si basa sull'IAM governando chi dovrebbe avere accesso a cosa nel tempo. Mentre l'IAM crea identità e accessi, l'IGA garantisce che tali diritti di accesso rimangano appropriati e conformi man mano che l'organizzazione e i ruoli evolvono. In altre parole, "assicura che l'accesso sia appropriato nel tempo gestendo le autorizzazioni, conducendo revisioni degli accessi e applicando controlli basati su policy".

In termini pratici, l'IGA comprende processi come la certificazione periodica degli accessi da parte dei manager, flussi di approvazione per le richieste di accesso, politiche di segregazione dei compiti per prevenire combinazioni di permessi rischiose e audit dei dati di identità.

Perché è importante: L'IGA è fondamentale per conformità, sicurezza ed efficienza. Senza governance, gli utenti accumulano privilegi eccessivi o mantengono accessi a sistemi che non servono più (ad esempio, dopo un cambio di ruolo o la cessazione del rapporto di lavoro). Questo "abuso di privilegi" crea vulnerabilità di sicurezza e può portare a fallimenti negli audit e nella conformità. L'IGA aiuta le organizzazioni ad applicare il principio del minimo privilegio – ogni identità con l'accesso strettamente necessario – e fornisce evidenze per le normative (come GDPR e NIS2) che l'accesso ai dati sensibili è correttamente controllato e revisionato. Automatizzando revisioni e approvazioni degli accessi, l'IGA riduce anche il carico manuale su IT e manager, rendendo la gestione degli accessi più scalabile.

In sintesi, l'IGA risponde alla domanda: "Questa identità dovrebbe ancora avere questo accesso?" in modo continuativo, mitigando minacce interne ed errori e garantendo che l'organizzazione rimanga sicura e pronta per gli audit.

Gestione degli accessi privilegiati (PAM)

La gestione degli accessi privilegiati (Privileged Access Management, PAM) è un'area specializzata di identity security focalizzata sugli account ad alto impatto – le "chiavi del regno". Gli account privilegiati (come amministratori di sistema, domain admin, proprietari di piattaforme cloud o account di servizio con ampie autorizzazioni) hanno capacità che, se vengono utilizzate in modo improprio o compromesse, potrebbero essere devastanti.

La PAM "si concentra sulla protezione delle credenziali ad alto rischio e delle autorizzazioni a livello amministrativo, che appartengano a un amministratore umano o a un account di servizio che controlla i sistemi di produzione".

I controlli chiave di PAM includono: archiviazione sicura delle credenziali privilegiate (ad esempio, in vault crittografati), accesso just-in-time (concessione di privilegi elevati solo quando necessario e per un tempo limitato), autenticazione multifattore per azioni privilegiate, monitoraggio e registrazione delle sessioni, logout automatico o rotazione delle credenziali dopo l'uso.

Perché è importante: Gli account privilegiati sono un obiettivo comune negli attacchi informatici: gli aggressori li cercano perché conferiscono il massimo livello di accesso.Senza PAM, una singola password di amministratore rubata può scatenare una violazione catastrofica, consentendo a un intruso di interrompere i sistemi o esfiltrare enormi quantità di dati. Le soluzioni PAM riducono significativamente questo rischio impedendo l'uso incontrollato di account potenti.

Esse garantiscono che gli amministratori utilizzino credenziali uniche e robuste (spesso concesse solo per la durata di un'attività) e che tutte le attività privilegiate siano tracciabili. Questo non solo ostacola gli attacchi esterni, ma mitiga anche le minacce interne o l'uso improprio accidentale da parte del personale IT.

Per l'organizzazione, implementare PAM significa che i sistemi e i dati critici sono molto meglio protetti da abusi. Inoltre, molti regimi di conformità richiedono esplicitamente controlli sull'accesso amministrativo: PAM aiuta a soddisfare tali requisiti attraverso supervisione e tracciabilità. In sintesi, PAM aggiunge un livello di sicurezza essenziale attorno agli accessi più sensibili, limitando drasticamente i danni che possono derivare da un'identità compromessa o utilizzata in modo improprio.

Strong Authentication e Access Control

Un'autenticazione efficace è alla base di tutti i domini di identity security sopra citati. L'autenticazione è il processo di verifica che un utente o un sistema sia realmente chi dichiara di essere. Un'autenticazione debole (come l'affidarsi esclusivamente alle password) è un punto noto di vulnerabilità: le password possono essere indovinate, rubate o ottenute tramite phishing.

Un'autenticazione forte (Strong Authentication) significa richiedere più fattori (MFA) o metodi moderni che gli attaccanti non possano facilmente aggirare. Per gli utenti umani, questo può includere codici monouso, app di autenticazione su smartphone, chiavi di sicurezza fisiche o dati biometrici, in aggiunta o in sostituzione della password.

Per le identità di sistema (come API o account di servizio), l'autenticazione forte implica eliminare le password statiche e utilizzare certificati o metodi basati su token con una gestione sicura delle chiavi.

Perché è importante: Secondo Microsoft, l'autenticazione multifattore (multifactor authentication, MFA) può prevenire il 99,9% degli attacchi di compromissione degli account utente. Implementando la MFA in tutta l'organizzazione, il rischio di accesso non autorizzato diminuisce drasticamente: anche se una password viene rubata, l'attaccante non può facilmente fornire il secondo fattore.

In termini di business, un'autenticazione forte è una delle misure di sicurezza con il ROI più alto: difende direttamente dagli attacchi comuni come phishing e credential stuffing, prevenendo così violazioni costose. Inoltre, tecniche come il conditional access (una policy di accesso che si adatta in base al contesto/rischio) rafforzano ulteriormente l'autenticazione.

Ad esempio, se un tentativo di login proviene da una posizione insolita o da un dispositivo non sicuro, il sistema può richiedere una verifica aggiuntiva o bloccare l'accesso. Questo garantisce sicurezza senza ostacolare inutilmente gli utenti legittimi.
Adottando il principio del "never trust" di default e verificando sempre l'identità in modo continuo (un pilastro dell'approccio Zero Trust), le organizzazioni possono abilitare con fiducia il lavoro da remoto e l'adozione del cloud. L'autenticazione forte e i controlli di accesso adattivi proteggono il business mentre garantiscono flessibilità: dipendenti, partner e clienti possono connettersi da qualsiasi luogo, ma alle condizioni dell'IT e con attrito minimo.

Identity Threat Detection and Response (ITDR)

Anche con misure preventive in atto, le organizzazioni devono assumere che alcune violazioni di identità possano verificarsi (ad esempio, un'email di phishing inganna un dipendente o un account legacy viene compromesso). Identity Threat Detection and Response (ITDR) è un pilastro emergente focalizzato sul rilevamento e la mitigazione degli attacchi incentrati sull'identità in tempo reale.

Esso "monitora l'uso improprio e la compromissione delle identità", osservando pattern anomali che indicano un impersonamento o un utilizzo non autorizzato delle credenziali. Questo può includere strumenti che analizzano il comportamento di login per individuare anomalie (viaggi impossibili, orari insoliti, cambiamenti nei dispositivi o negli schemi IP), rilevano attacchi all'infrastruttura di directory (come escalation di privilegi in Active Directory o abuso di token SSO) e si integrano con le operazioni di sicurezza più ampie per rispondere alle minacce che prendono di mira le identità.

Perché è importante: Il monitoraggio tradizionale della sicurezza si è concentrato su endpoint e reti, ma gli attaccanti moderni spesso li aggirano sfruttando le debolezze dell'identità – ad esempio, utilizzando credenziali valide per accedere e poi elevando i privilegi in modo silenzioso. Le soluzioni ITDR colmano questa lacuna fornendo rilevamento specifico per gli attacchi basati sull'identità, che potrebbero non generare allarmi negli strumenti per endpoint o rete.

Gartner e i leader del settore sottolineano ITDR come componente cruciale di una strategia Zero Trust, garantendo che comportamenti sospetti da parte di o contro un'identità vengano intercettati tempestivamente. Ad esempio, se un attaccante ottiene accesso a un account inattivo e inizia ad accedere a dati sensibili, ITDR può segnalare questa attività anomala e automatizzare la risposta (come revocare i token o richiedere una nuova autenticazione).

L'approccio di Microsoft a ITDR evidenzia l'integrazione tra protezione dell'identità e operazioni di sicurezza – condividendo segnali tra i sistemi di identità e il Security Operations Centre (SOC) per bloccare rapidamente gli attacchi.

In termini di business, le capacità ITDR riducono la probabilità che una violazione dell'identità si trasformi in un incidente su larga scala. Aiutano a limitare il livello di impatto ("blast radius") di una compromissione rilevandola rapidamente e rispondendo (spesso in modo automatico) prima che l'attaccante possa muoversi più in profondità nei sistemi. Come parte di un programma maturo di identity security, ITDR offre a CISO e CIO maggiore fiducia che, anche se i controlli preventivi falliscono, esista una rete di sicurezza per intercettare e contenere le minacce basate sull'identità.

Creare un programma completo di Identity Security

Comprendere i componenti è solo l'inizio – ma come integrarli in modo strategico? Un programma di identity security di successo riguarda tanto le persone e i processi quanto la tecnologia. Ecco i passaggi chiave e le best practice per implementare un programma olistico:

Valutare e inventariare tutte le identità e gli accessi Non puoi proteggere ciò che non conosci. Inizia con una scoperta approfondita delle identità umane e non umane presenti nella tua organizzazione (account del personale, account di servizio, ruoli cloud, ecc.) e dei relativi accessi. Identifica le identità ad alto rischio (come i domain admin o gli account di fornitori terzi) e gli account "orfani" non associati a un proprietario attuale Questa valutazione rivelerà lacune, come utenti con permessi eccessivi o applicazioni senza MFA, e guiderà le priorità. Utilizzare gli strumenti giusti può trasformare questo processo da un lavoro manuale su fogli di calcolo a un'attività ripetibile e automatizzata.

Applicare un'autenticazione forte ovunque: Rendi obbligatoria la multi-factor authentication (MFA) per tutti gli utenti, in particolare per gli accessi privilegiati e remoti. Considera l'introduzione graduale di metodi avanzati come l'autenticazione passwordless (es. biometria o chiavi di sicurezza FIDO2) per una maggiore sicurezza e usabilità. Utilizza policy di conditional access per adattarti al rischio – ad esempio, richiedi MFA solo per applicazioni sensibili o quando vengono rilevati indicatori di rischio (posizioni di login insolite, viaggi impossibili). Questo garantisce che le misure di sicurezza restino efficaci senza generare affaticamento negli utenti.

Adottare il principio del least privilege tramite processi IAM & IGA: Sfrutta i tuoi strumenti di IAM e IGA per applicare il principio secondo cui ogni identità ottiene il minimo accesso necessario. Definisci controlli di accesso basati sui ruoli (RBAC) in modo che i ruoli standard abbiano accessi predefiniti, riducendo concessioni di privilegi ad hoc. Implementa un processo di identity lifecycle: quando le persone entrano, cambiano ruolo o lasciano l'organizzazione, i loro accessi devono essere aggiornati o rimossi tempestivamente. Esegui regolarmente revisioni degli accessi (attestazioni) per i sistemi critici – utilizzando soluzioni IGA per far certificare a manager o proprietari dei sistemi chi deve mantenere l'accesso. Questo ciclo di governance previene il privilege creep e garantisce la conformità nel tempo.

Proteggi e controlla gli accessi privilegiati: Se non l'hai già fatto, valuta l'investimento in una soluzione PAM o sfrutta le funzionalità di gestione privilegiata nel cloud (come Microsoft Entra Privileged Identity Management per i ruoli di Azure AD). Archivia tutte le password amministrative in vault e utilizza processi di check-out con approvazioni per chiunque ottenga accesso elevato. Abilita l'elevazione just-in-time affinché i diritti amministrativi scadano automaticamente quando non sono in uso. Monitora tutte le sessioni amministrative (registrando i comandi o le sequenze di tasti per i server critici, se possibile) e configura alert per attività privilegiate insolite (es. aggiunta imprevista di un nuovo utente al gruppo domain admins). Tratta la tua infrastruttura di directory (es. Active Directory o Entra ID) come un asset di Tier 0 – proteggila con i controlli di sicurezza più elevati, poiché tutti gli altri accessi dipendono dalla sua integrità.

Integrare i segnali di identità nel rilevamento delle minacce: Invia i log delle attività di identità (provenienti da sistemi IAM, Active Directory, directory cloud, SSO, ecc.) nei flussi di lavoro del tuo Security Operations (SIEM/SOC). Implementa strumenti di rilevamento delle minacce basate sull'identità – ad esempio Microsoft Entra ID Protection e Microsoft Defender for Identity – specializzati nell'individuare attacchi alle credenziali o utilizzi anomali. Assicurati che, quando viene rilevata una potenziale compromissione, esistano playbook per rispondere rapidamente: automatizza la disabilitazione degli account o il reset delle password per gli account sospetti, e sfrutta il conditional access per bloccare dinamicamente o richiedere autenticazioni aggiuntive per sessioni rischiose. Simula regolarmente scenari di violazione dell'identità per testare il rilevamento e la risposta (ad esempio, esegui un drill di phishing e verifica se il SOC intercetta l'uso di una credenziale di test compromessa).

Promuovere una cultura orientata alla sicurezza: La tecnologia da sola non basta. Educa i dipendenti sulle buone pratiche di igiene dell'identità – come riconoscere tentativi di phishing, utilizzare password manager approvati e non condividere mai le credenziali. Definisci policy e formazione affinché tutti comprendano che proteggere il proprio login è parte della loro responsabilità (ad esempio, segnalare immediatamente dispositivi smarriti o non ignorare i prompt MFA). Costruisci una partnership tra gli amministratori delle identità e il team di sicurezza: devono lavorare fianco a fianco, poiché l'identità è ora una linea di difesa primaria. Quando i team IT e sicurezza collaborano (come incoraggiato nell'architettura di riferimento Microsoft), le minacce possono essere affrontate più rapidamente e le policy perfezionate continuamente. Seguendo queste pratiche, le organizzazioni creano più livelli di difesa attorno alle identità mantenendo l'accesso agile. L'obiettivo è una postura di identity security adattiva e resiliente – che non solo protegge dagli attacchi alle credenziali di oggi, ma si adatta alle nuove minacce e alle esigenze aziendali nel tempo.

Questo approccio completo trasforma identity security da una sfida complessa a un abilitatore del business: consentendo alle persone giuste di connettersi alle risorse giuste in modo sicuro e bloccando gli attaccanti all'ingresso.

Identity Maturity

Gestita
Provisioning automatizzato. SSO su tutte le principali applicazioni, controlli sugli accessi privilegiati, revisioni degli accessi di routine

Base
Directory centralizzate, MFA per alcuni utenti, accesso basato su ruoli (RBAC) di base, audit occasionali

Ottimizzata
Policy di accesso condizionale, identity-based threat detection, processi di governance solidi

Ad hoc
Sistemi disconnessi, scarsa igiene delle password, provisioning degli utenti manuale, implementazione minima o assente di MFA

Adattiva
Accesso basato sul rischio (Risk-driven access), passwordless, rilevamento basato su AI (AI-powered detection), allineamento con Zero Trust e gli obiettivi di business

Il futuro della Identity Security

La Identity security non è più soltanto un meccanismo di controllo dell'accesso ai sistemi: sta diventando una piattaforma dinamica e intelligente che abilita una collaborazione sicura, un accesso decentralizzato e processi automatizzati su larga scala. Con la crescita del cloud, del lavoro ibrido e delle operazioni basate sull'intelligenza artificiale, il ruolo dell'identità evolve da semplice presidio reattivo a elemento di difesa proattiva e vero abilitatore del business. Le organizzazioni più lungimiranti stanno già preparando le fondamenta per questa trasformazione.

Ecco le tendenze che stanno plasmando il futuro della Identity Security – e cosa significano per la tua organizzazione.

Identità decentralizzata e Credenziali Verificabili

L'Identità Decentralizzata (Decentralised Identity, DID) consente agli utenti di gestire e controllare i propri dati identificativi senza fare affidamento su un'autorità centrale. Le identità sono costruite attorno a credenziali verificabili, archiviate off-chain in portafogli digitali sicuri e validate tramite crittografia a chiave pubblica o registri distribuiti. Microsoft sta investendo in questo ambito attraverso Entra Verified ID, supportando la transizione verso un modello di identità self-sovereign.

Perché è importante: questo modello riduce la dipendenza dai provider di identità e consente alle organizzazioni di validare attributi identificativi (ad esempio stato occupazionale, certificazioni, stato di salute) senza archiviare dati personali. In settori come l'istruzione, la pubblica amministrazione e la sanità, migliora la privacy, previene le frodi legate all'identità e semplifica la conformità a normative come il GDPR. Con la crescente adozione, le organizzazioni dovranno sviluppare strategie per emettere, verificare e utilizzare credenziali decentralizzate in modo sicuro e su larga scala.

Identity-as-Code e Accesso basato su Policy

Ispirato al modello infrastructure-as-code, l'approccio identity-as-code tratta le configurazioni di identità (ruoli, policy, autorizzazioni) come codice sotto controllo di versione, integrato nelle pipeline CI/CD. Strumenti come Microsoft Entra Permissions Management e framework di governance basati su Terraform stanno portando questo concetto nel mainstream degli ambienti enterprise.

Perché è importante: definire le policy di identità come codice consente implementazioni più rapide, coerenti e facilmente verificabili. Permette ai team di sicurezza e piattaforma di collaborare tramite workflow DevSecOps, riducendo errori umani e configurazioni errate. Man mano che le organizzazioni scalano verso ambienti multi-cloud e ibridi, l'identity-as-code garantisce che i controlli di accesso evolvano insieme all'infrastruttura, e non in un secondo momento.

Esplosione delle Machine Identity

Le identità non umane – API, container, dispositivi IoT, microservizi – superano ormai il numero degli utenti umani nella maggior parte delle aziende. Ognuna di queste identità richiede credenziali (token, secret, certificati) e controlli di accesso. Tuttavia, molte organizzazioni continuano a considerarle un elemento secondario, con credenziali hardcoded, rotazione insufficiente o assenza di gestione del ciclo di vita.

Perché è importante: le machine identity rappresentano un fattore critico di rischio, frequentemente utilizzate per ottenere accessi prolungati e non rilevati. Una gestione efficace richiede controlli dedicati – tra cui rotazione automatizzata dei secret, visibilità sugli account di servizio inutilizzati o con privilegi eccessivi, e integrazione con strumenti di gestione dei secret (ad esempio Azure Key Vault, HashiCorp Vault). Nei programmi di identità moderni, identità umane e machine vengono governate con lo stesso rigore.

Protezione AI-Augmented delle Identità

L'intelligenza artificiale e il machine learning stanno diventando elementi chiave nella difesa delle identità digitali. Soluzioni come Microsoft Entra ID Protection e Defender for Identity sfruttano già l'AI per individuare comportamenti anomali negli accessi – ad esempio impossible travel, token replay o tentativi di MFA fatigue. Queste tecnologie stanno evolvendo rapidamente verso modelli decisionali sempre più autonomi e sensibili al contesto, capaci di riconoscere rischi emergenti e intervenire in modo proattivo, riducendo tempi di risposta e migliorando significativamente la postura di sicurezza.

Perché è importante: Le regole statiche non riescono a tenere il passo con la velocità e la creatività degli attaccanti moderni. La protezione basata sull'AI abilita una valutazione del rischio in tempo reale, policy adattive e remediation automatizzate – riducendo i tempi di risposta e limitando l'impatto di potenziali compromissioni. Con il miglioramento dei modelli AI, le piattaforme di identità gestiranno sempre più autonomamente il ciclo rileva-decidi-agisci, coinvolgendo gli analisti umani solo nei casi più critici o ambigui.

Insight & Microsoft: i tuoi partner per l'eccellenza nella Identity Security

Implementare l'intero spettro della sicurezza delle identità può essere complesso. È qui che il partner giusto può fare la differenza. Insight è riconosciuta come leader nei servizi di Identity Security, grazie a una partnership estremamente solida con Microsoft. Il team di esperti Insight vanta una profonda esperienza pratica nelle tecnologie Microsoft per identità e sicurezza – da Azure Active Directory (oggi Microsoft Entra ID) alle soluzioni più avanzate di identity governance e threat protection. Insight è inoltre uno dei principali partner globali di Microsoft nella sicurezza: possediamo tutte e quattro le Microsoft Security Advanced Specialisations, inclusa quella dedicata a Identity and Access Management, oltre alle specializzazioni in Cloud Security, Information Protection e Threat Protection. Insight fa anche parte della Microsoft Intelligent Security Association (MISA), collaborando a stretto contatto con i team di prodotto Microsoft dedicati alla sicurezza.

Cosa significano queste credenziali per un cliente? In parole semplici, Insight offre un'expertise comprovata nella progettazione e nell'implementazione di una strategia di sicurezza delle identità su misura per la tua organizzazione, sfruttando al massimo le tecnologie Microsoft. Che tu stia rafforzando l'infrastruttura di identità on-premises o adottando l'intera suite Microsoft Entra per la gestione cloud delle identità, Insight mette a disposizione oltre 1.500 architetti e ingegneri della sicurezza certificati Microsoft. I nostri esperti hanno supportato aziende in tutto il mondo nell'implementazione di multifactor authentication, single sign-on su migliaia di applicazioni, automazione del ciclo di vita delle identità tramite strumenti come Microsoft Entra ID Governance, integrazione dei segnali di identità nelle piattaforme di rilevamento delle minacce. Allineiamo queste soluzioni ai tuoi obiettivi di business, assicurando che i miglioramenti della sicurezza supportino anche la produttività e l'esperienza utente.

La collaborazione strategica tra Insight e Microsoft ci mantiene sempre all'avanguardia nelle nuove evoluzioni della sicurezza delle identità. Ad esempio, quando Microsoft ha introdotto le funzionalità di Identity Threat Detection & Response e le analisi di sicurezza basate sull'AI, Insight è stata tra le prime a integrare queste capacità nei propri servizi gestiti. Insight è stata anche tra le prime aziende a ottenere lo status Microsoft verified Managed XDR, a dimostrazione della nostra capacità di combinare il rilevamento delle minacce alle identità con operazioni di risposta attive 24/7. Inoltre, seguiamo la Microsoft Security Reference Architecture, un blueprint di best practice che garantisce che tutti i componenti della sicurezza delle identità si integrino perfettamente nel tuo ambiente. Il risultato è una soluzione coesa e armonizzata, non un insieme di strumenti isolati.

Soprattutto, Insight considera la sicurezza delle identità come un abilitatore strategico per il tuo business. Non ci limitiamo a implementare la tecnologia: collaboriamo con i tuoi stakeholder per sviluppare policy, modelli di governance e strategie di adozione da parte degli utenti che rendano le soluzioni davvero efficaci. Secondo il team di sicurezza di Insight UK, «l'identità digitale è la chiave per accedere al cuore di qualsiasi organizzazione e deve quindi essere protetta con la stessa priorità dei dati o dell'infrastruttura... Microsoft offre un'architettura completa, ma il vero impatto si ottiene quando viene combinata con cultura, processi e impegno organizzativo». Insight aiuta a riunire tutti questi elementi. Offriamo servizi che spaziano dalle valutazioni iniziali e workshop, all'implementazione pratica, fino ai servizi gestiti per la sicurezza delle identità. Indipendentemente dal punto in cui ti trovi nel tuo percorso di maturità in ambito identity security, Insight ha l'esperienza necessaria per guidarti avanti.

Scegliendo Insight come partner, ottieni un team non solo altamente competente dal punto di vista tecnico, ma anche profondamente impegnato nel tuo successo. Misuriamo il nostro successo in base alla tua capacità di prevenire violazioni, soddisfare i requisiti di conformità e adottare con sicurezza nuove tecnologie – il tutto supportato da un solido framework di sicurezza delle identità. Con Insight e Microsoft al tuo fianco, puoi trasformare la sicurezza delle identità da una preoccupazione a un punto di forza per il tuo business.

Microsoft

Conclusione

La Identity Security non è un semplice elemento da spuntare in una checklist: rappresenta un imperativo strategico nell'attuale scenario di rischio. Comprendendo e applicando i suoi pilastri fondamentali (IAM, IGA e ITDR), le organizzazioni possono proteggere i propri asset più critici e consentire alle persone di lavorare in modo efficiente e sicuro. Sebbene il percorso possa sembrare complesso, non è necessario affrontarlo da soli. Con un partner affidabile come Insight – che unisce tecnologie Microsoft leader di mercato a un'expertise consolidata – è possibile costruire un programma di sicurezza delle identità solido, capace di proteggere l'azienda oggi e prepararla alle sfide di domani.

Parla con un Identity Security Expert

Glossario

Termine	Definizione
Access Control	Policy e tecnologie che determinano chi può accedere a specifici sistemi, dati o servizi e a quali condizioni.
Authentication	Il processo di verifica dell'identità di un utente, dispositivo o sistema utilizzando fattori come password, dati biometrici o chiavi di sicurezza.
Authorisation	Il processo che determina cosa un'identità autenticata è autorizzata a fare o a quali risorse può accedere.
Conditional Access	Policy di accesso dinamiche che valutano segnali di rischio (come stato del dispositivo o posizione) prima di concedere l'accesso.
Decentralised Identity (DID)	Un modello di identità in cui gli individui controllano i propri dati e le proprie credenziali, verificate tramite tecnologie distribuite.
Directory Services	Sistemi centralizzati per la gestione delle informazioni di identità, come Microsoft Entra ID o Active Directory.
Identity and Access Management (IAM)	Sistemi e policy fondamentali per gestire le identità digitali e controllare l'accesso alle risorse.
Identity-as-Code	Trattare le configurazioni di identità (ruoli, policy) come codice, per automatizzazione, verificabilità e integrazione nelle pipeline DevOps.
Identity Governance and Administration (IGA)	Strumenti e processi per gestire il ciclo di vita degli accessi, incluse revisioni, approvazioni e applicazione delle policy.
Identity Lifecycle	L'intero processo di onboarding, modifica e offboarding delle identità durante il loro ciclo di vita in azienda.
Identity Threat Detection and Response (ITDR)	Funzionalità che monitorano e rispondono a minacce basate sull'identità, come abuso, escalation o rilevamento di anomalie.
Just-in-Time (JIT) Access	Concessione di accessi privilegiati in modo temporaneo e solo quando necessario, per ridurre al minimo i rischi permanenti.

Termine	Definizione
Least Privilege	Principio secondo cui utenti e sistemi devono avere solo i permessi necessari per svolgere il proprio lavoro – niente di più.
Machine Identity	Identità non umane utilizzate da software, API, servizi o dispositivi, che richiedono controlli e una governance specifica.
Multifactor Authentication (MFA)	Un metodo di autenticazione che richiede due o più forme di verifica, migliorando la resistenza ai tentativi di compromissione degli account.
Passwordless Authentication	Metodi di accesso che eliminano la necessità di password, utilizzando biometria, dispositivi attendibili o chiavi crittografiche.
Privileged Access Management (PAM)	Controlli e strumenti che proteggono account amministrativi e altri account sensibili tramite vaulting, monitoraggio e accesso Just-in-Time.
Role-Based Access Control (RBAC)	Metodo per assegnare i diritti di accesso in base alla funzione o al ruolo dell'utente.
Self-Sovereign Identity (SSI)	Un modello in cui gli utenti possiedono e gestiscono le proprie identità digitali in modo indipendente dalle autorità centrali.
Service Account	Identità digitale utilizzata da sistemi o software per eseguire attività automatizzate, spesso con privilegi elevati.
Single Sign-On (SSO)	Sistema che consente agli utenti di autenticarsi una sola volta e ottenere accesso a più applicazioni o sistemi.
Token-Based Authentication	Autenticazione basata su token sicuri (ad es. JWT), invece di reinserire nome utente e password.
Zero Trust	Filosofia di sicurezza moderna secondo cui l'accesso non è mai dato per scontato e deve essere sempre verificato, basandosi sul contesto e su una valutazione continua.

Passi Successivi

Contatta Insight per costruire un programma completo di sicurezza delle identità. Poiché oggi l'identità è il principale vettore di attacco per le aziende, proteggere ogni utente, account di servizio e connessione è una missione critica. Il nostro approccio olistico protegge le identità digitali, riduce il rischio e abilita i principi Zero Trust. Ti aiutiamo a garantire che solo le persone giuste ottengano il livello di accesso corretto, semplificando al tempo stesso la produttività. Affidati alla profonda esperienza di Insight e alla partnership con Microsoft per trasformare la sicurezza delle identità da una sfida complessa a un vero abilitatore di business.

- **it.insight.com**
- **02 21080210**