Preparato per

KEEPER

Beyond the Vault:
migliorare la gestione degli accessi privilegiati nelle aziende moderne

Luglio 2025 White Paper EMA
di **Ken Buckler, CASP;** Direttore della ricerca,
Sicurezza delle informazioni, rischio e gestione della conformità

EMA™
IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

Indice

Introduzione

In un'era di minacce informatiche incessanti e di rapida trasformazione digitale, la gestione degli accessi privilegiati (PAM) è emersa come una disciplina di sicurezza fondamentale. Le aziende di oggi richiedono molto di più del vaulting delle credenziali; richiedono un framework completo che protegga le risorse critiche, applichi l'accesso con privilegi minimi e si integri perfettamente in ambienti on-premise e cloud.

Un PAM efficace inizia con una solida verifica dell'identità e un'autenticazione multifattoriale per combinare token hardware, approvazioni mobili e controlli biometrici supportati da crittografia end-to-end e sicurezza zero-knowledge. I controlli granulari basati sui ruoli e provisioning just-in-time all'interno di un'architettura zero-trust garantiscono che gli utenti ricevano i privilegi minimi necessari, riducendo drasticamente l'impatto delle violazioni. Allo stesso tempo, i registri di audit catturano ogni sessione privilegiata, dai comandi eseguiti alle riproduzioni visive e alla durata della sessione. I log di audit alimentano quindi i motori di conformità automatizzati che allineano le pratiche agli standard HIPAA, SOX e PCI DSS, mentre le campagne di ricertificazione eliminano gli account orfani o eccessivi.

È essenziale una perfetta integrazione con i servizi cloud e gli strumenti esistenti. L'iniezione delle credenziali in script, pipeline e gateway di accesso remoto mantiene la produttività degli utenti senza sacrificare il controllo. L'analisi comportamentale avanzata e l'agentic AI elevano quindi il PAM a una difesa attiva. Gli avvisi e le azioni in tempo reale possono terminare le minacce e revocare i privilegi istantaneamente. Estendere questi controlli a terze parti tramite la condivisione vincolata al tempo e ai dispositivi, la rotazione automatica delle password e i rigidi flussi di lavoro di approvazione mitiga ulteriormente i rischi per gli appaltatori e la catena di fornitura.

In questo white paper, esamineremo le sfide che le organizzazioni devono affrontare per soddisfare queste priorità PAM e valuteremo come la piattaforma KeeperPAM di Keeper Security si confronta con il settore in generale.

Zero Trust by Design

Zero trust e zero knowledge

La nostra soluzione utilizza lo zero-trust per progettazione

Integrare i principi di zero-trust fin dall'inizio non è più facoltativo per la gestione degli accessi privilegiati; è fondamentale. Un framework "zero-trust per progettazione" tratta ogni richiesta di privilegi elevati come intrinsecamente non affidabile, richiedendo una verifica continua, una segmentazione rigorosa e l'applicazione del principio del minimo privilegio. Passando da credenziali statiche e onnipotenti a token di accesso temporanei e sensibili al contesto, le organizzazioni possono ridurre drasticamente la superficie di attacco e limitare i movimenti laterali in caso di violazione. Con lo zero-trust per progettazione, ogni decisione di accesso considera l'identità dell'utente, la postura del dispositivo, la posizione, l'ora del giorno e il contesto comportamentale. Il provisioning just-in-time garantisce che i diritti privilegiati siano concessi solo per la durata esatta necessaria e revocati automaticamente in seguito. I controlli di accesso capillari e basati sui ruoli riducono al minimo le autorizzazioni eccessive, mentre l'autenticazione a più fattori e il monitoraggio continuo delle sessioni proteggono dalla compromissione delle credenziali e dalle minacce interne.

"\[Quando si tratta di gestione degli accessi privilegiati, le nostre priorità sono\] l'integrazione con l'architettura zero trust e il framework di convalida continua".
- Direttore IT, 500–749 dipendenti, che utilizza KeeperPAM

L'approccio zero-knowledge di Keeper alla progettazione del prodotto migliora ulteriormente questo approccio, che garantisce che tutta la crittografia e la decrittografia avvengano localmente sul tuo dispositivo: solo il testo cifrato arriva al cloud di Keeper. Una password principale e qualsiasi materiale chiave derivato non escono mai dal dispositivo scelto, il che significa che i server di Keeper non

possono accedere o archiviare dati non crittografati o le chiavi che li proteggono. Anche se la loro infrastruttura venisse violata, gli aggressori otterrebbero solo una stringa di caratteri illeggibile, garantendo una vera riservatezza end-to-end.

I dati del sondaggio sottolineano l'impatto di questo approccio: il 60% degli utenti di Keeper Security considera la propria implementazione PAM come "zero-knowledge" e "zero-trust per progettazione", rispetto ad appena il 34,9% degli utenti di tutti gli altri fornitori. Questa differenza riflette un atteggiamento di sicurezza proattivo: i clienti di Keeper sottolineano la convalida continua, l'eliminazione degli account condivisi e la gestione automatizzata del ciclo di vita dei privilegi, rispetto a una mentalità più reattiva e orientata alla conformità altrove.

Il PAM zero-trust accelera anche la conformità e la prontezza per gli audit. Ogni sessione privilegiata viene registrata dall'inizio alla fine, completa di comandi eseguiti, riproduzione visiva e metriche di durata, alimentando motori di conformità automatizzati allineati ai requisiti HIPAA, SOX e PCI DSS. In pratica, le organizzazioni che integrano il modello zero trust nelle loro architetture PAM non solo rafforzano le difese, ma semplificano anche le operazioni, riducono i costi associati agli account orfani e dimostrano miglioramenti misurabili nel contenimento delle violazioni.

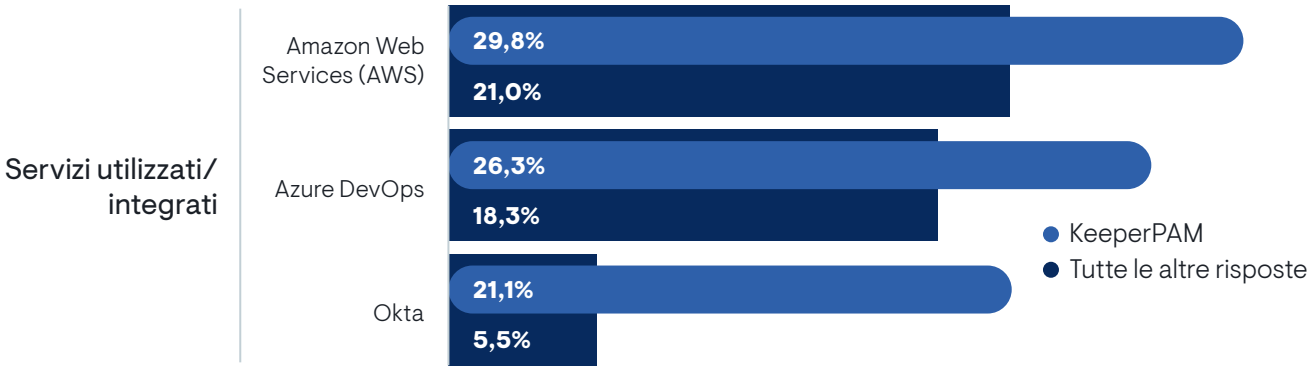
In definitiva, l'approccio zero-knowledge e il design zero-trust di Keeper trasformano l'accesso privilegiato da una potenziale responsabilità in un processo controllato e verificabile, che si adatta in tempo reale ai rischi in evoluzione e garantisce che i sistemi critici rimangano sicuri, conformi e resilienti.

Facilità di distribuzione, configurazione e integrazioni

Non esiste una scorciatoia, ma Keeper ci va vicino

La facilità di implementazione, configurazione e integrazione può determinare il successo o il fallimento del ROI di un progetto PAM. Secondo il sondaggio dell'EMA, il 60% dei clienti di Keeper Security ha valutato l'implementazione iniziale come "molto semplice", rispetto a solo il 22,1% degli utenti su altre piattaforme PAM. Al contrario, il 10% dei clienti di tutte le altre soluzioni ha definito l'implementazione "difficile" o "molto difficile", un punto dolente del tutto assente tra gli utenti di KeeperPAM. La migrazione degli strumenti PAM legacy e on-premise al cloud è ancora un ostacolo per il 39% delle organizzazioni, una complessità che l'architettura nativa del cloud di Keeper evita. Gli ostacoli all'integrazione affliggono l'11% delle implementazioni non-Keeper, in cui sono spesso necessari connettori proprietari e script manuali per integrarsi con pipeline SIEM, di ticketing o DevOps. Le API modulari di KeeperPAM, i connettori plug-and-play e l'orchestrazione cloud senza interruzioni accelerano il time-to-value e riducono al minimo gli attriti operativi.

Gioca bene con gli altri



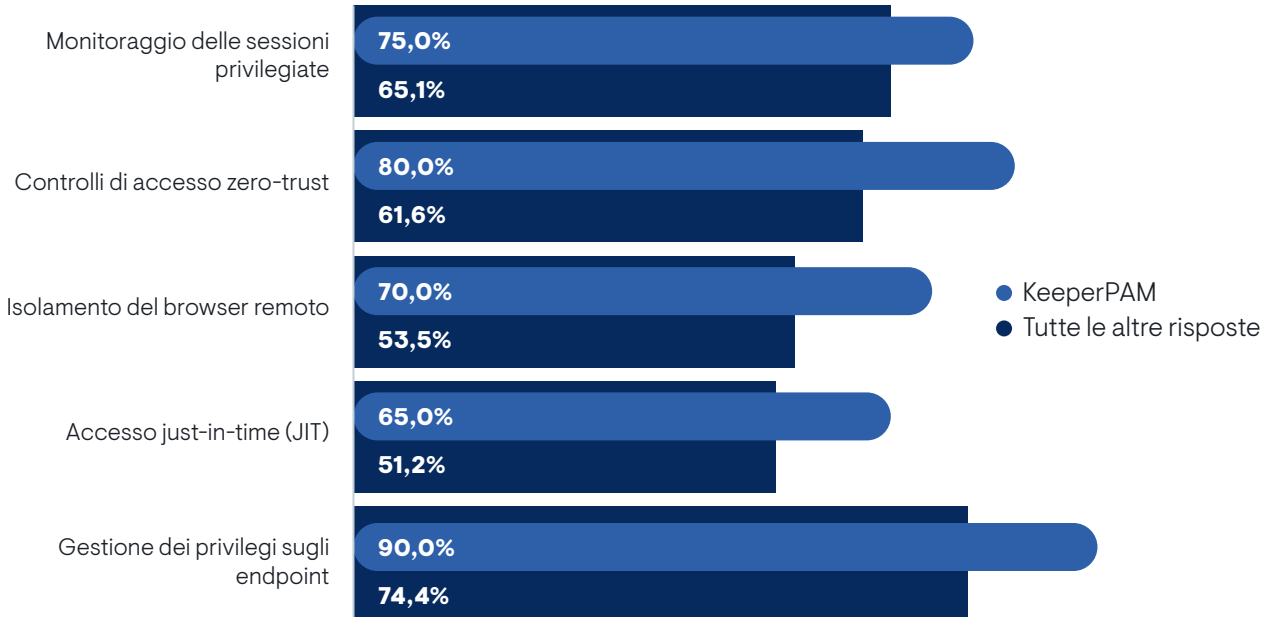
Le integrazioni perfette sono una pietra miliare di qualsiasi strategia PAM moderna e anche in questo caso Keeper è all'avanguardia. I connettori e le API predefiniti consentono un'integrazione rapida e bidirezionale con le piattaforme principali, avviando istanze EC2 in Amazon Web Services, automatizzando le pipeline in Azure DevOps o centralizzando l'autenticazione tramite Okta. Gli utenti di KeeperPAM riportano un'adozione molto più alta di queste integrazioni rispetto ad altre soluzioni PAM, eliminando la necessità di script personalizzati dispendiosi in termini di tempo o di manutenzione manuale dei connettori. Integrando l'iniezione di credenziali privilegiate direttamente nei flussi di lavoro CI/CD, nelle console cloud e nei provider di identità, KeeperPAM riduce al minimo gli attriti, aumenta la produttività degli sviluppatori e garantisce che i segreti rimangano protetti a ogni livello.

Fare Di Più con Meno Personale

I requisiti di personale per le implementazioni di PAM variano ampiamente a seconda della piattaforma. Solo il 15% dei clienti di Keeper Security dichiara di aver bisogno di personale dedicato per gestire l'implementazione, la configurazione e l'integrazione, grazie all'interfaccia utente intuitiva di Keeper, alle procedure guidate di configurazione e alla documentazione completa. Al contrario, il 39,5% delle organizzazioni che utilizzano altre soluzioni PAM necessita di uno o più amministratori a tempo pieno per mantenere in funzione i propri ambienti. Questi team spesso si destreggiano tra la complessa manutenzione dei dispositivi on-premise, scripting su misura e aggiornamenti manuali dei connettori, aumentando il personale e mettendo sotto pressione le risorse IT esistenti. Il design cloud native e gli strumenti self-service di Keeper riducono al minimo la necessità di competenze specializzate. Gli amministratori possono integrare nuovi sistemi, regolare le politiche dei privilegi e integrarsi con le pipeline SIEM o DevOps senza pesanti personalizzazioni. In definitiva, una riduzione dei costi del personale si traduce in implementazioni più rapide e operazioni a lungo termine più sostenibili e convenienti.

Oltre la gestione di password e chiavi segrete

Funzionalità PAM avanzate



Il PAM moderno richiede molto più della semplice archiviazione delle credenziali: necessita di un ricco set di funzionalità che difende, monitora e si adatta attivamente alle minacce in evoluzione. KeeperPAM si distingue offrendo capacità avanzate che molti fornitori tradizionali semplicemente non offrono o non implementano su larga scala. Il monitoraggio delle sessioni privilegiate, ad esempio, è cruciale per catturare ogni sequenza di tasti, comando e riproduzione visiva delle attività ad alto rischio. I clienti di Keeper sfruttano questa funzione più frequentemente rispetto ai loro pari, consentendo il rilevamento delle minacce in tempo reale e l'analisi forense.

"L'utilizzo di PAM rafforza l'integrità dei nostri dati e la nostra reputazione".
- VP Development/Engineering, 1.000-2.499 dipendenti, usando KeeperPAM

L'accesso alla rete zero-trust estende i principi del privilegio minimo oltre le password a ogni richiesta di accesso. Keeper incorpora controlli contestuali delle policy (postura del dispositivo, posizione, ora e linee di base comportamentali) assicurando che anche le sessioni autenticate rimangano sotto controllo continuo. Questo controllo granulare delle operazioni privilegiate riduce drasticamente la potenziale finestra di esposizione rispetto ai modelli statici, tutto o niente.

L'isolamento remoto del browser (RBI) è un'altra area in cui Keeper supera la concorrenza. Inoltrando le console di amministrazione attraverso browser isolati e sicuri, le organizzazioni eliminano l'accesso diretto agli endpoint per terze parti e appaltatori, isolando efficacemente potenziali malware o furti di credenziali. Poche altre soluzioni PAM integrano RBI così senza intoppi, costringendo invece a soluzioni manuali che compromettono sia la sicurezza che l'esperienza dell'utente.

Il provisioning just-in-time e la gestione automatizzata del ciclo di vita dei privilegi completano il toolkit avanzato di Keeper. L'elevazione temporanea e limitata nel tempo impedisce l'accumulo di account con privilegi elevati, mentre le campagne automatiche di deprovisioning e ricertificazione assicurano il rispetto dei mandati di conformità senza oneri manuali. Infine, la gestione dei privilegi degli endpoint, rimuovendo i diritti di amministratore locale e concedendo privilegi limitati su richiesta, protegge sia dagli attacchi esterni che dall'uso improprio interno.

Andando oltre le password e i segreti, Keeper trasforma PAM in una piattaforma di difesa attiva: una piattaforma che anticipa gli attacchi, applica lo zero-trust a ogni livello e fornisce i controlli avanzati richiesti dagli ambienti complessi di oggi.

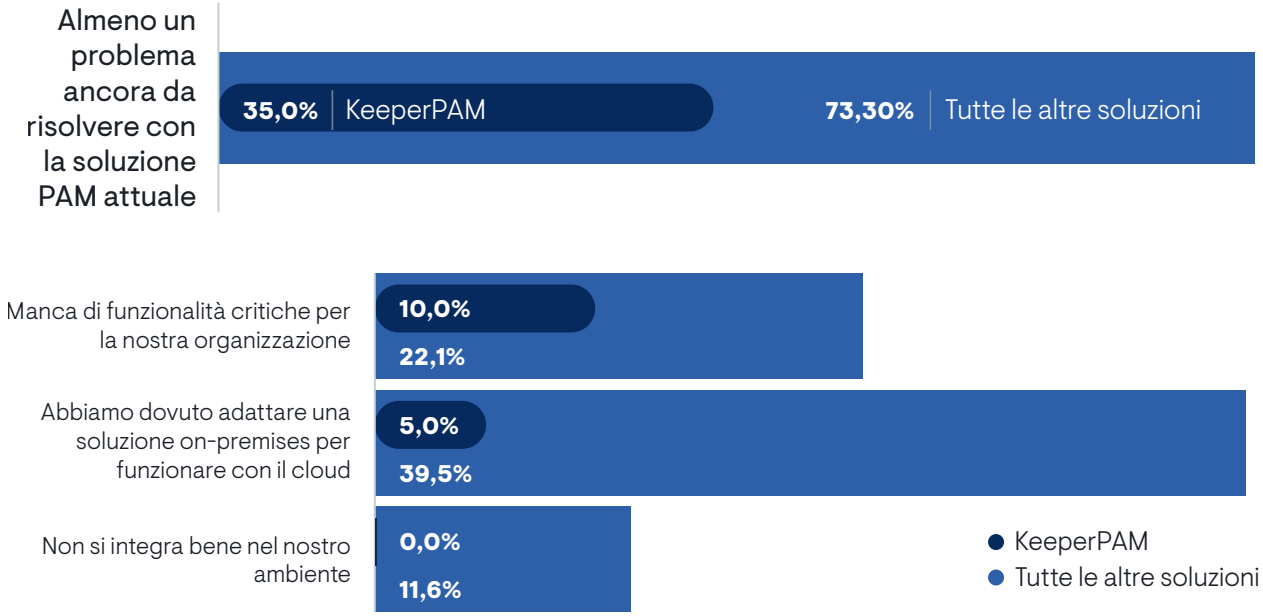
Soddisfazione complessiva

La soluzione PAM è pronta per affrontare qualsiasi tempesta?

La soddisfazione dei clienti è il metro di misura più importante per capire quanto vale una soluzione PAM e quanto dura nel tempo. Quando il 5% delle organizzazioni che utilizzano altre piattaforme è attivamente alla ricerca di un sostituto, segnala lacune critiche in affidabilità, usabilità e/o supporto. Al contrario, nessun utente di Keeper Security ha segnalato l'intenzione di abbandonare il proprio strumento PAM, sottolineando la capacità di Keeper di soddisfare le esigenze di sicurezza e operative in continua evoluzione.

Inoltre, il 75% dei clienti di Keeper si definisce complessivamente "molto soddisfatto", superando di gran lunga il 53,5% di utenti di fornitori concorrenti che si dichiarano "molto soddisfatti". Un'elevata soddisfazione è correlata a un'adozione più rapida, una riduzione del rischio più efficace e un costo totale di proprietà inferiore, poiché i team soddisfatti investono in integrazioni più profonde e funzionalità più avanzate. In un panorama in cui l'accesso privilegiato è continuamente preso di mira, scegliere una piattaforma che delizia i suoi utenti non è solo un vantaggio, è fondamentale per la missione.

Le funzionalità e le integrazioni sono punti critici fondamentali



Nonostante il loro ruolo critico, molte implementazioni di PAM si scontrano con ostacoli persistenti. Il 73% delle organizzazioni che utilizzano soluzioni non Keeper segnala almeno una sfida significativa, rispetto a solo il 35% dei clienti Keeper. I punti dolenti comuni includono la mancanza di capacità essenziali, costringendo i team a integrare strumenti di terze parti, la scarsa integrazione nell'infrastruttura esistente e il problema di adattare le piattaforme locali per supportare gli ambienti cloud. Gli utenti di KeeperPAM riscontrano questi problemi molto meno frequentemente, grazie al suo set completo di funzionalità, all'architettura nativa cloud-first e all'ampia libreria di connettori. Riducendo al minimo le lacune funzionali e semplificando le implementazioni ibride, Keeper non solo accelera il time-to-value, ma riduce anche il carico di lavoro legato alla risoluzione dei problemi e alle soluzioni alternative, permettendo ai team di sicurezza di concentrarsi sulla mitigazione proattiva dei rischi piuttosto che sulla gestione delle limitazioni legacy.

Soluzione migliore, priorità migliori

Altre implementazioni PAM non riescono a sfruttare appieno il loro potenziale

Area prioritaria	Clienti Keeper	Altre soluzioni PAM
Autenticazione	Continua, zero-trust	Basato sui ruoli, MFA
Gestione credenziali	Elimina le credenziali statiche/condivise	Controllo di base e accesso al monitoraggio
Formazione	Priorità esplicita	Non enfatizzato
Automazione	Focus sulla mitigazione del rischio (perché il	Process efficiency focus
processo è già efficiente)	Focus sull'efficienza dei processi	Minimum regulatory compliance
Conformità	Uso improprio delle credenziali e attenzione all'audit	Conformità normativa minima

Keeper Security consente alle organizzazioni di passare da una modalità di manutenzione e conformità a un atteggiamento proattivo e orientato alla sicurezza. I clienti di KeeperPAM eliminano le credenziali statiche e condivise in modo non sicuro attraverso un motore di archiviazione a conoscenza zero che emette segreti effimeri e con privilegi minimi, riducendo drasticamente sia i vettori di attacco esterni che gli abusi interni rispetto agli approcci tradizionali basati esclusivamente su vault. L'autenticazione continua e i controlli di accesso zero-trust, inclusi i controlli sullo stato dei dispositivi, la geolocalizzazione e l'analisi comportamentale, garantiscono che ogni sessione rimanga sotto controllo molto tempo dopo un prompt MFA una tantum, rendendo praticamente impossibile per gli aggressori sfruttare le credenziali rubate senza essere scoperti. L'automazione incentrata sul rischio di Keeper gestisce l'intero ciclo di vita dei privilegi, dalla scoperta e dall'integrazione fino a rotazione e deprovisioning automatici, prevenendo la proliferazione delle credenziali e gli account orfani, mentre molte altre soluzioni si limitano ad automatizzare i flussi di lavoro di approvazione o i report di conformità. È importante sottolineare che i clienti di Keeper integrano esplicitamente la formazione e la sensibilizzazione del

personale come controllo di sicurezza fondamentale, riconoscendo che i fattori umani sono cruciali quanto la tecnologia nel promuovere l'adozione e prevenire soluzioni alternative rischiose.

"Penso che il monitoraggio costante degli account privilegiati mi aiuti a dormire meglio la notte".
– Vicepresidente Sviluppo/Ingegneria, 2.500-4.999 dipendenti, con KeeperPAM

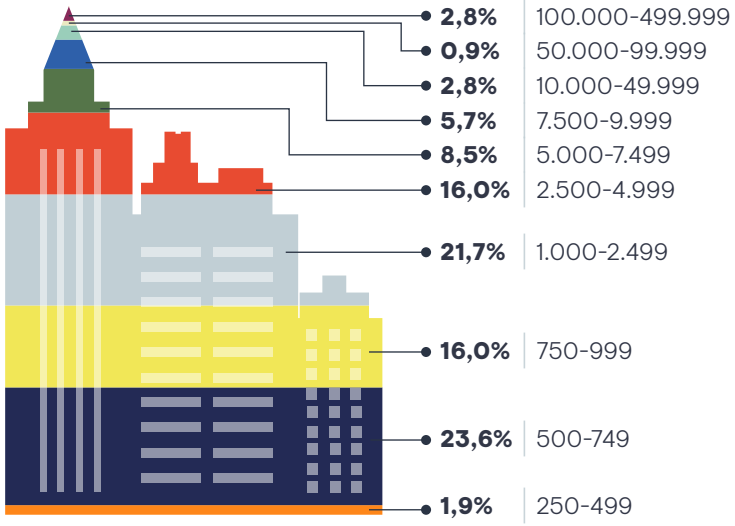
Al contrario, gli utenti di altri strumenti PAM spesso enfatizzano i controlli tradizionali, come l'accesso basato sui ruoli, l'auditing post-accesso e l'efficienza operativa, riflettendo una mentalità reattiva che lotta con le lacune di funzionalità, le integrazioni fragili e la complessità del retrofit delle soluzioni on-premise per il cloud. L'architettura cloud native di Keeper e l'ampia libreria di connettori plug-and-play eliminano questi problemi, consentendo un'integrazione rapida con piattaforme SIEM, provider di identità come Okta e pipeline CI/CD in AWS o Azure DevOps. Le funzionalità avanzate, tra cui il monitoraggio delle sessioni privilegiate, l'isolamento remoto del browser, il provisioning just-in-time e la gestione dei privilegi degli endpoint, sono tutte native di Keeper, riducendo gli attriti di implementazione e le continue richieste di personale.

Combinando queste funzionalità di nuova generazione con un'esperienza utente senza interruzioni, Keeper consente ai team di sicurezza di anticipare le minacce, applicare una protezione continua e rafforzare davvero il loro ambiente di accesso privilegiato.

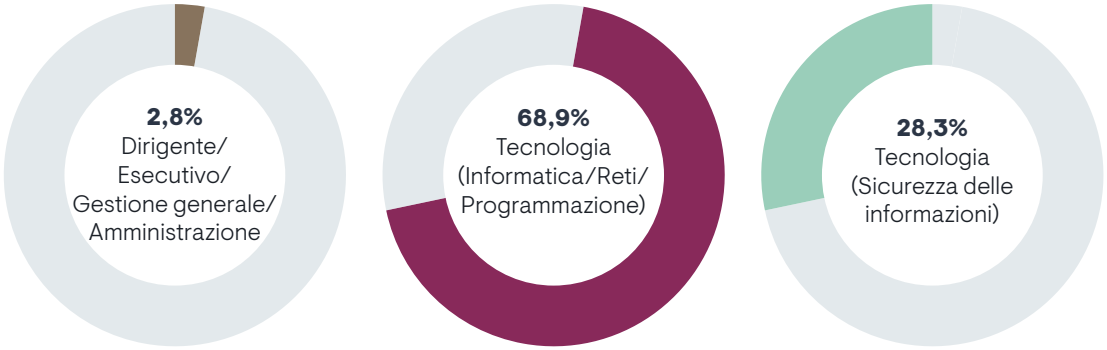
Metodologia

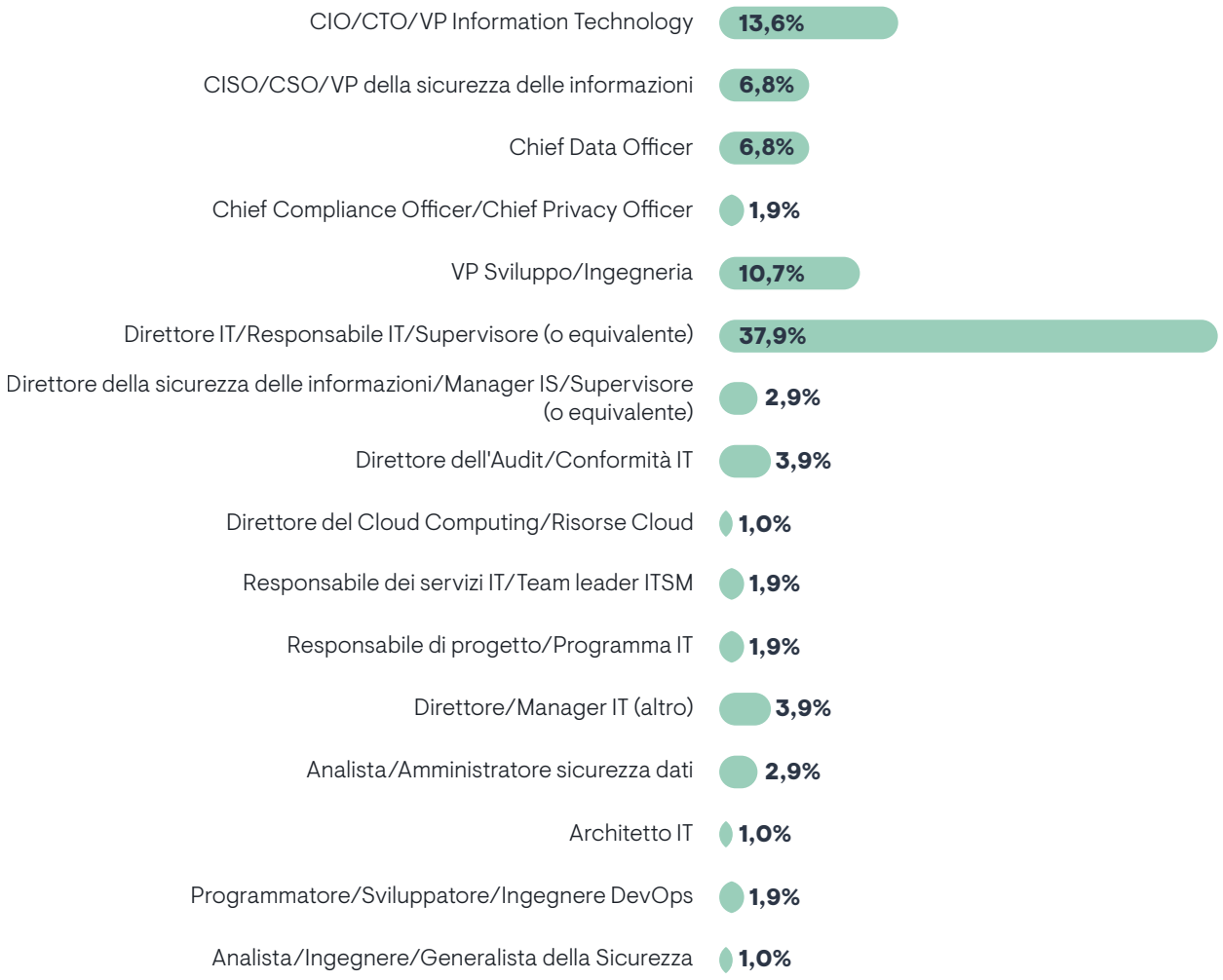
Totale di 106 professionisti che utilizzano BeyondTrust, CyberArk, Delinea, Devolutions, Keeper Security, ManageEngine, One Identity o StrongDM a partire da giugno 2025. Tutti i dati di questo white paper si basano sulle risposte al sondaggio e sulle risposte aperte riguardanti le priorità e le sfide della gestione degli accessi privilegiati nell'impresa.

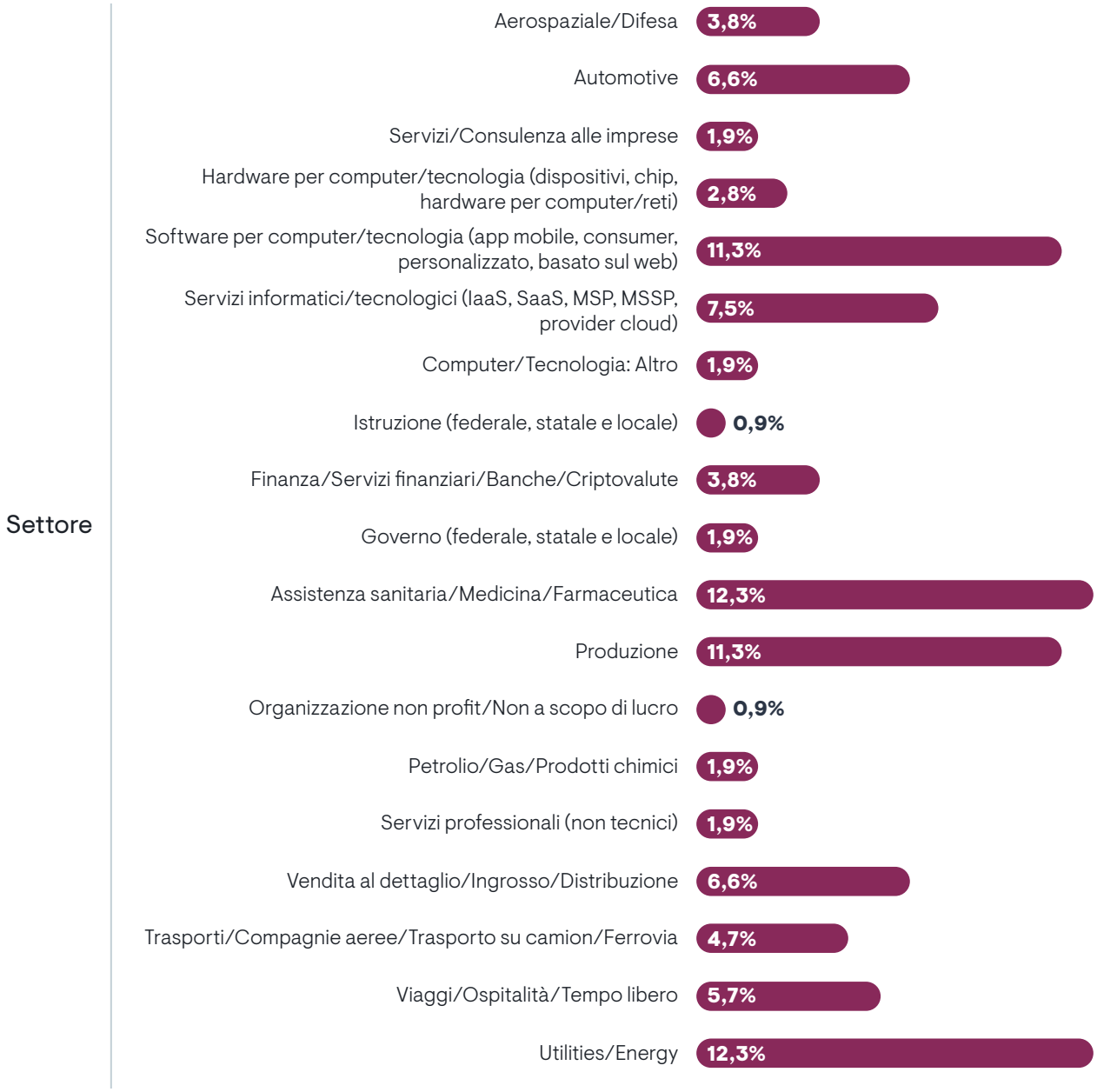
Dimensioni dell'organizzazione



Ruolo del rispondente




CIO/CTO/VP Information Technology
13,6%
CISO/CSO/VP della sicurezza delle informazioni
6,8%
Chief Data Officer
6,8%
Chief Compliance Officer/Chief Privacy Officer
1,9%
VP Sviluppo/Ingegneria
10,7%
Direttore IT/Responsabile IT/Supervisore (o equivalente)
37,9%
Direttore della sicurezza delle informazioni/Manager IS/Supervisore (o equivalente)
2,9%
Direttore dell'Audit/Conformità IT
3,9%
Direttore del Cloud Computing/Risorse Cloud
1,0%
Responsabile dei servizi IT/Team leader ITSM
1,9%
Responsabile di progetto/Programma IT
1,9%
Direttore/Manager IT (altro)
3,9%
Analista/Amministratore sicurezza dati
2,9%
Architetto IT
1,0%
Programmatore/Sviluppatore/Ingegnere DevOps
1,9%
Analista/Ingegnere/Generalista della Sicurezza
1,0%


Settore
Aerospaziale/Difesa 3,8%
Automotive 6,6%
Servizi/Consulenza alle imprese 1,9%
Hardware per computer/tecnologia (dispositivi, chip, hardware per computer/reti) 2,8%
Software per computer/tecnologia (app mobile, consumer, personalizzato, basato sul web) 11,3%
Servizi informatici/tecnologici (IaaS, SaaS, MSP, MSSP, provider cloud) 7,5%
Computer/Tecnologia: Altro 1,9%
Istruzione (federale, statale e locale) 0,9%
Finanza/Servizi finanziari/Banche/Criptovalute 3,8%
Governo (federale, statale e locale) 1,9%
Assistenza sanitaria/Medicina/Farmaceutica 12,3%
Produzione 11,3%
Organizzazione non profit/Non a scopo di lucro 0,9%
Petrolio/Gas/Prodotti chimici 1,9%
Servizi professionali (non tecnici) 1,9%
Vendita al dettaglio/Ingrosso/Distribuzione 6,6%
Trasporti/Compagnie aeree/Trasporto su camion/Ferrovia 4,7%
Viaggi/Ospitalità/Tempo libero 5,7%
Utilities/Energy 12,3%

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading IT research and consulting firm dedicated to delivering actionable insights across the evolving technology landscape. Through independent research, market analysis, and vendor evaluations, we empower organizations to make well-informed technology decisions. Our team of analysts combines practical experience with a deep understanding of industry best practices and emerging vendor solutions to help clients achieve their strategic objectives. Learn more about EMA research, analysis, and consulting services at **www.enterprisemanagement.com** or follow EMA on **X** or **LinkedIn**.

2770 Arapahoe Road, Ste 132 - 544, Lafayette, CO 80026 +1 303.543.9500 **www.enterprisemanagement.com**

4577.081325-IT