



Implementa policy di accesso a privilegi minimi, elimina i diritti amministrativi permanenti e abilita l'accesso Just-in-Time (JIT) sia a livello di processo sia di macchina con la gestione dei privilegi degli endpoint su Windows, Linux e macOS.

**I controlli di accesso privilegiati robusti sono essenziali affinché le organizzazioni possano rafforzare il proprio livello di sicurezza, garantire l'efficienza operativa e rispettare i requisiti di conformità normativa.**

Keeper Endpoint Privilege Manager protegge gli endpoint attraverso agenti leggeri che rimuovono i diritti di amministrazione permanenti, consentendo l'elevazione temporanea dei privilegi in base alle policy solo quando necessario. Il sistema applica politiche di sicurezza personalizzabili tramite accesso JIT con flussi di lavoro di approvazione opzionali e applicazione dell'autenticazione a più fattori (MFA).

Le azioni privilegiate possono essere eseguite tramite account temporanei che vengono creati e rimossi automaticamente per ogni sessione, oppure elevando temporaneamente i privilegi sugli account utente standard. Le organizzazioni possono scegliere uno dei due metodi a seconda del proprio livello di sicurezza e delle esigenze operative.

Keeper Endpoint Privilege Manager funziona su ambienti Windows, macOS e Linux, offrendo visibilità attraverso una dashboard centralizzata che registra tutte le attività di elevazione per audit e conformità.

## Vantaggi di Keeper Endpoint Privilege Manager

### Sicurezza

Elimina i diritti di amministratore permanenti e consente l'elevazione just-in-time solo per le applicazioni approvate, per ridurre le superfici di attacco e migliorare la sicurezza.

### Conformità

Offre tracce di audit complete sull'uso dei privilegi e garantisce il rispetto dei requisiti normativi attraverso un controllo documentato degli accessi amministrativi.

### Efficienza operativa

Riduce il workload dell'help desk automatizzando le approvazioni per le attività amministrative di routine.

### Esperienza utente

Consente agli utenti di completare le attività necessarie senza ritardi IT grazie all'elevazione automatica dei privilegi per le applicazioni approvate.

### Scalabilità

Consente alle organizzazioni di applicare in modo efficiente policy di privilegi minimi e di gestire l'accesso con privilegi su migliaia di endpoint Windows, macOS e Linux da una piattaforma centralizzata.

### Audit e visibilità

Fornisce approfondimenti sull'attività di elevazione, sulle approvazioni e sull'applicazione delle policy degli endpoint con registrazioni dettagliate e integrazione negli strumenti SIEM per una risposta più rapida agli incidenti.

Saperne di più  
[keepersecurity.com](https://keepersecurity.com)

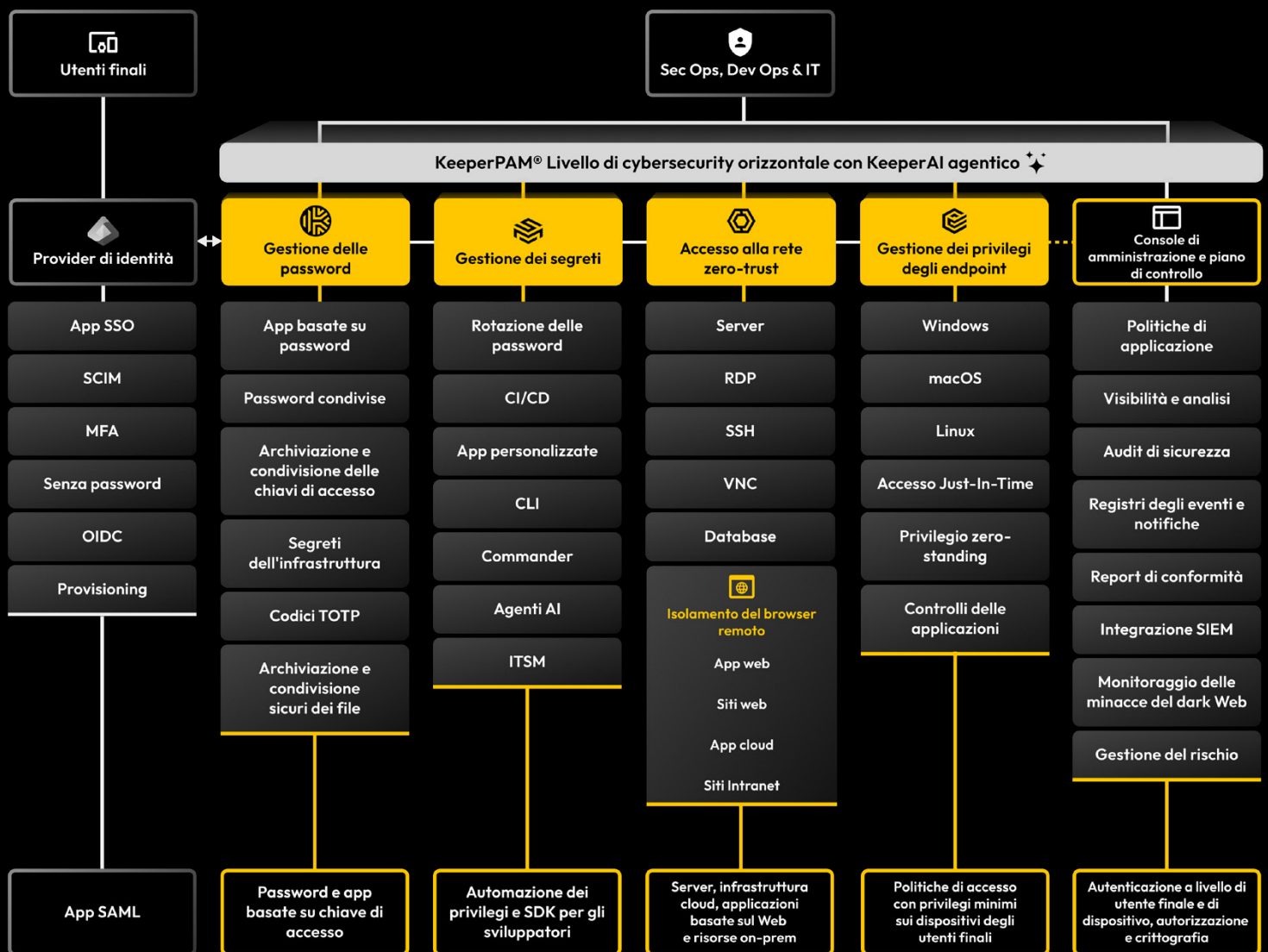
Richiedi una demo  
[keeper.io/demo](https://keeper.io/demo)

Richieste dei partner  
[partners@keepersecurity.com](mailto:partners@keepersecurity.com)



## Informazioni su Keeper Security

Keeper Security sta trasformando la sicurezza informatica per persone e organizzazioni in tutto il mondo. Le soluzioni intuitive di Keeper sono basate sulla crittografia end-to-end per proteggere ogni utente, su ogni dispositivo, in ogni luogo. Scelto da milioni di persone e migliaia di organizzazioni, Keeper è leader nella gestione degli accessi privilegiati.



## Estendi zero trust agli endpoint

Endpoint Privilege Manager estende l'approccio zero-trust di KeeperPAM controllando l'elevazione dei privilegi direttamente sugli endpoint, integrando le funzionalità di connessione sicura della soluzione PAM più ampia. Mentre il resto della piattaforma KeeperPAM protegge le modalità di connessione degli utenti ai sistemi, Endpoint Privilege Manager regola i diritti amministrativi che gli utenti possono esercitare una volta connessi.

## In che modo Keeper eleva i privilegi

- 1. Policy** - se un'applicazione o un processo richiede l'elevazione, l'agente di Keeper verifica la policy pertinente.
- 2. Approvazione** - se è richiesta l'approvazione, la richiesta viene inoltrata a un amministratore tramite la console di amministrazione o l'interfaccia della riga di comando (CLI)
- 3. Opzione MFA** - se non è necessaria alcuna approvazione, l'elevazione procede automaticamente. L'applicazione dell'MFA è un passaggio aggiuntivo opzionale