

Mettiamo in sicurezza le identità e gli accessi privilegiati con la soluzione

ManageEngine 
PAM360

ManageEngine

DISTRIBUTED BY

BLUDIS
VALUE ADDED DISTRIBUTOR

✓ SCELTO DA OLTRE 280.000
AZIENDE IN TUTTO IL MONDO

✓ UTILIZZATO DA 9 SU 10 DELLE
SOCIETÀ "FORTUNE 100"

✓ SCELTO DA OLTRE 3 MILIONI DI
AMMINISTRATORI IT

✓ 15 ANNI DA DISTRIBUTORE UNICO
ITALIANO MANAGEENGINE

✓ 28 ANNI DI ESPERIENZA NEL
SETTORE ICT

✓ NEXT GEN VENDOR DISTRIBUTOR
DEL GRUPPO ESPRINET

BLUDIS
VALUE ADDED DISTRIBUTOR

ManageEngine

Mettiamo in sicurezza le identità e gli accessi privilegiati con la soluzione PAM360 di ManageEngine

Le credenziali privilegiate, rappresentando le chiavi per l'accesso e per la gestione degli asset critici aziendali, sono il principale target dei cyber attacchi attuali.

Le aziende dovrebbero dotarsi di strumenti per monitorare e gestire gli account privilegiati che accedono alle risorse IT dell'organizzazione e le attività ad esse associate.

Nel corso dell'intervento sarà presentata la soluzione PAM360 di ManageEngine e come attraverso il suo utilizzo sia possibile prevenire gli attacchi informatici consentendo alle aziende di proteggere i sistemi e i processi business-critical.

Speaker

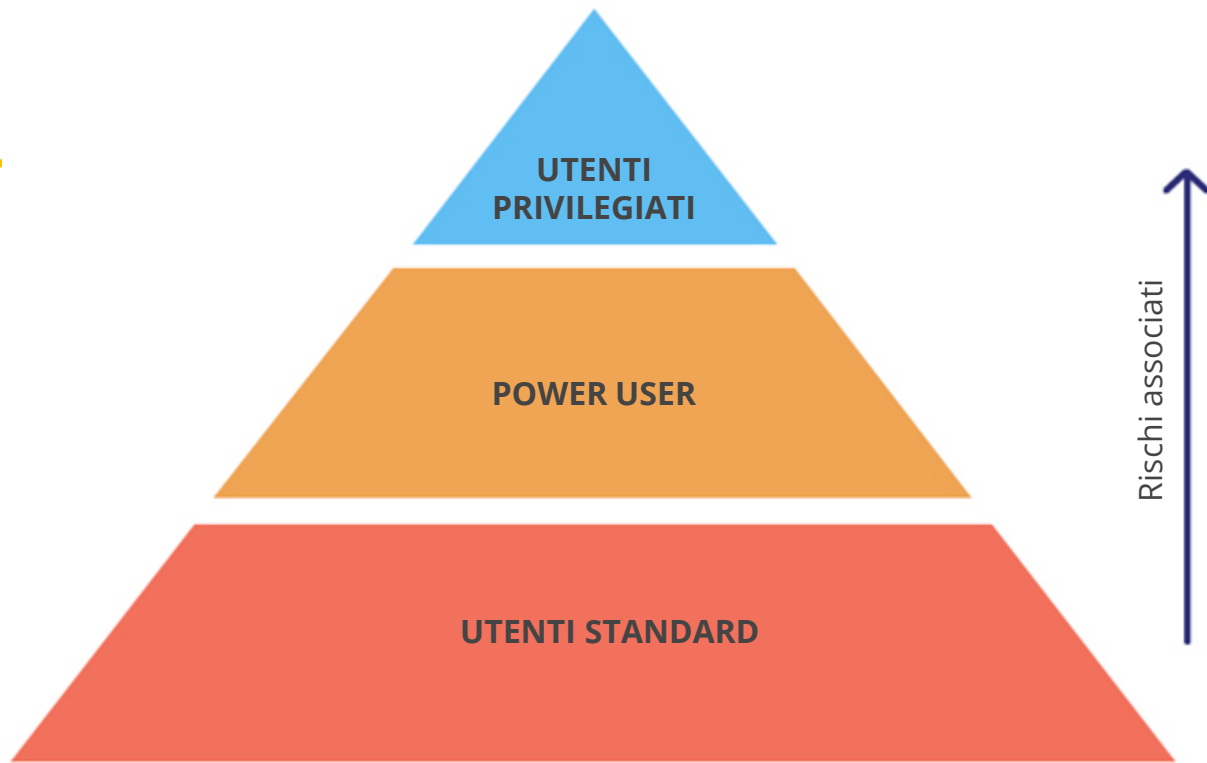


Andrea Balestrero

Sales Engineer ManageEngine

Identità e Accessi privilegiati





Tipologie di utenti IT in una azienda

Cyber attacks



Attaccante



Opzione 2 - Attacco indiretto, sfrutta l'utente muovendosi lateralmente tra le risorse

Opzione 1 - Attacco diretto, meno comune negli anni recenti



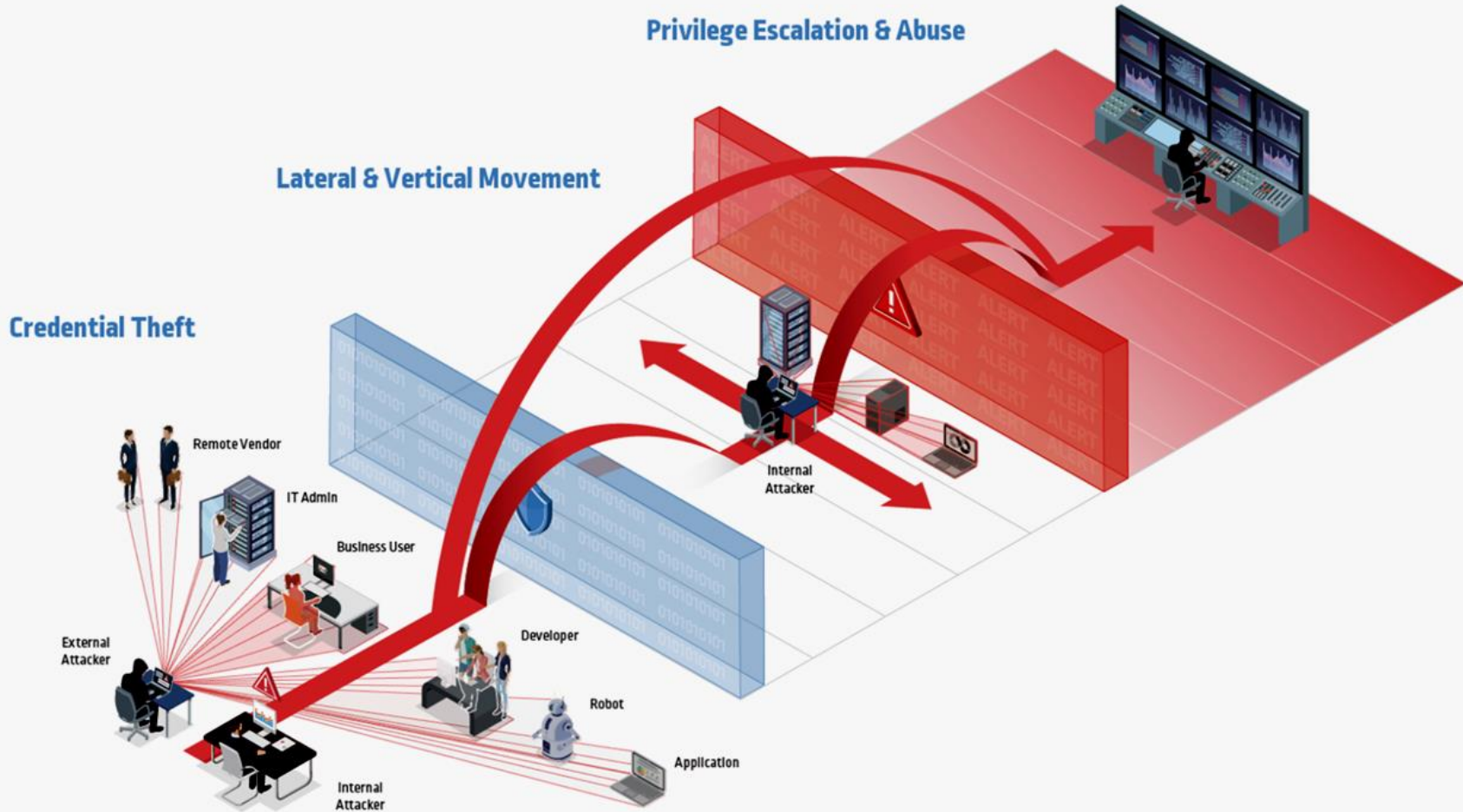
Utente privilegiato



Spostamento laterale e sfruttamento di vulnerabilità o vettori di attacco privilegiati

Risorse sensibili





La soluzione completa per la gestione degli accessi privilegiati

Piattaforma di Privileged Access Management di controllo accessi e monitoraggio delle attività degli utenti privilegiati per l'accesso alle risorse critiche aziendali.

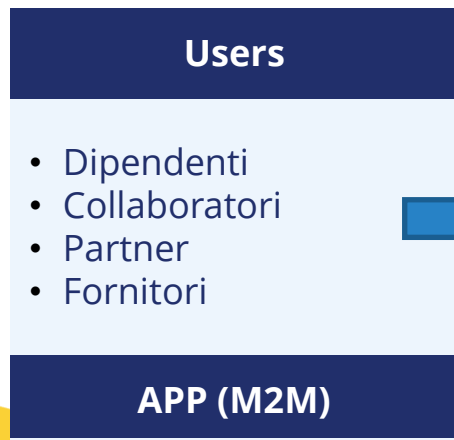
PAM360 permette di rispondere a queste domande

- Conosci il numero di credenziali privilegiate che la tua organizzazione utilizza
- Conosci su quali risorse aziendali questi account privilegiati vengono utilizzati
- Conosci chi ha accesso ed utilizza questi account privilegiati
- Come vengono condivise tra le persone?
- Cosa succede quando qualcuno che conosce tutte le password lascia l'azienda?
- Come tieni traccia dei tuoi certificati SSL e delle loro date di scadenza?
- Hai un sistema di gestione dei certificati digitali?
- Come gestisci le chiavi SSH?

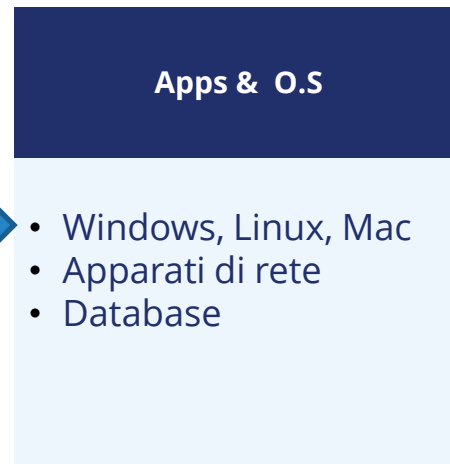
PAM360 permette di gestire questi scenari

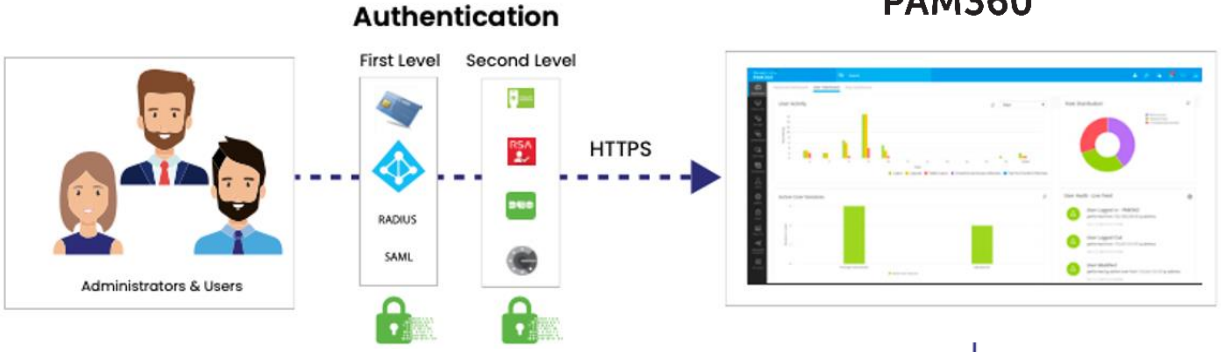
- Local Administrator uguale su tutti i sistemi stessa password
- Proliferazione degli account active directory privilegiati:
- Nessun inventory degli account e credenziali privilegiate
- Nessun sistema di monitoraggio e di controllo dell'accesso ad account e credenziali privilegiate
- Nessun sistema di monitoraggio e di controllo delle attività privilegiate

Il contesto applicativo di ManageEngine PAM360

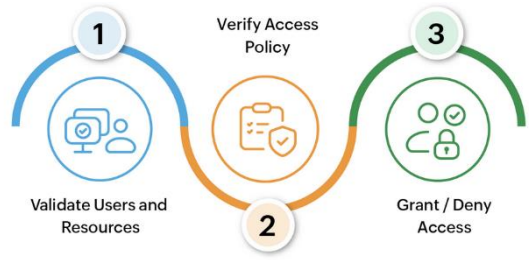


ManageEngine
PAM360





Zero Trust Approach in PAM360



Zero Trust - Policy-Based Access Privilege

ManageEngine PAM360

Search

Trust Score

User Trust Score

Resource Trust Score

Authentication Device

Overall User Trust Score (%)

Category	Score
Authentication	9
Authentication	5
Authentication	7
Authentication	4
Authentication	6
Authentication	5
Device	9
Device	5
Device	6
Device	8
Device	7
Device	4
Device	3
Device	6
Device	7
Device	7

Authentication-36.00% Device-64.00%

Overall User Trust Score (%)

Authentication and Device share details

100%

Authentication Device

Password Protected Device : 10

Firewall Enabled : 4

Allowed OS Version : 5

Allowed Open Ports : 3

Allowed Browser Plugins/Addons : 7

Secure Boot Enabled : 7

Allowed Applications/Packages : 9

Driver Integrity Verification Available : 8

Allowed Process/Services : 8

Active Antivirus Software : 8

Note: All entries will have a preset value of 10 points by default. However, the Admin can modify the points as per priority.

Save Cancel

PAM360 approccio alla gestione degli accessi e identità

Zero trust



Principle of least privileges (PoLP)
(principio del privilegio minimo)



L'approccio Zero Trust alla sicurezza degli accessi privilegiati

ManageEngine
PAM360



Elevazione dei privilegi just-in-time

Assegna privilegi solo per un determinato periodo e per una specifica attività



Accesso remoto sicuro

Accesso ai sistemi remoti attraverso gateway con sessioni crittografate e sicure



Smart workflow per il controllo degli accessi

Controllo degli accessi basato su ruolo (RBAC) e workflow avanzato su richiesta

Mettere in pratica lo Zero Trust con ManageEngine

Scenari reali

BLUDIS
VALUE ADDED DISTRIBUTOR

ManageEngine

Un ingegnere di rete in vacanza



SCENARIO

Un ingegnere di rete in vacanza cerca di accedere al firewall aziendale ed effettuare modifiche alla configurazione, al fine di validare un indirizzo IP.

Nel farlo, l'ingegnere utilizza i suoi dispositivi personali connessi alla Wi-fi dell'hotel dove risiede in quel momento.

COME AFFRONTARLO



- Autenticati in una soluzione PAM tramite MFA
- Fa una richiesta per l'accesso ai firewall aziendale e attendi l'approvazione
- Stabilisci un accesso limitato (30-45 minuti) con revoca automatica dopo il tempo stabilito
- Accesso remoto da fornire tramite getaway/proxy senza rivelare le credenziali

Come può aiutarti ManageEngine

Password Request

Resource Name : centos6 Account Name : root

Access request for the password will be sent to admin and the approval status will be mailed back to MDaniels@cyber.com. You must specify the reason for access along with the access request.

You want to access the password : Now Later

From : 24/07/2019

Start Time : 15 : 50 hours

To : 24/07/2019

End Time : 15 : 50 hours

Current time in the server: 15:48 hours

A reminder mail will be sent to you 15 minutes prior to the start of access time.

Comments :

Send Cancel

Assegnazione del privilegio just-in-time
Richiedi l'accesso alle risorse per un determinato periodo

Il Database Administrator che lavora da remoto



SCENARIO

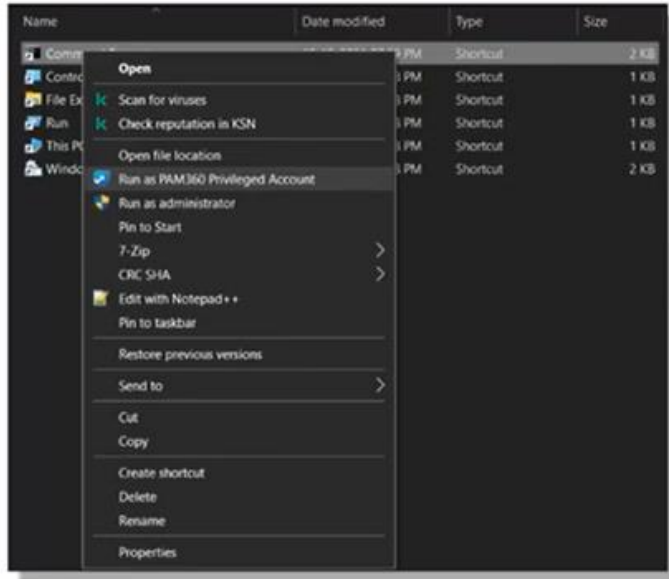
Un Database Administrator (DBA) che lavora da remoto ha costante necessità di accedere al database SQL interno all'azienda, i cui dipendenti lavorano in prevalenza da coffee shops cambiando spesso device.



COME AFFRONTARLO

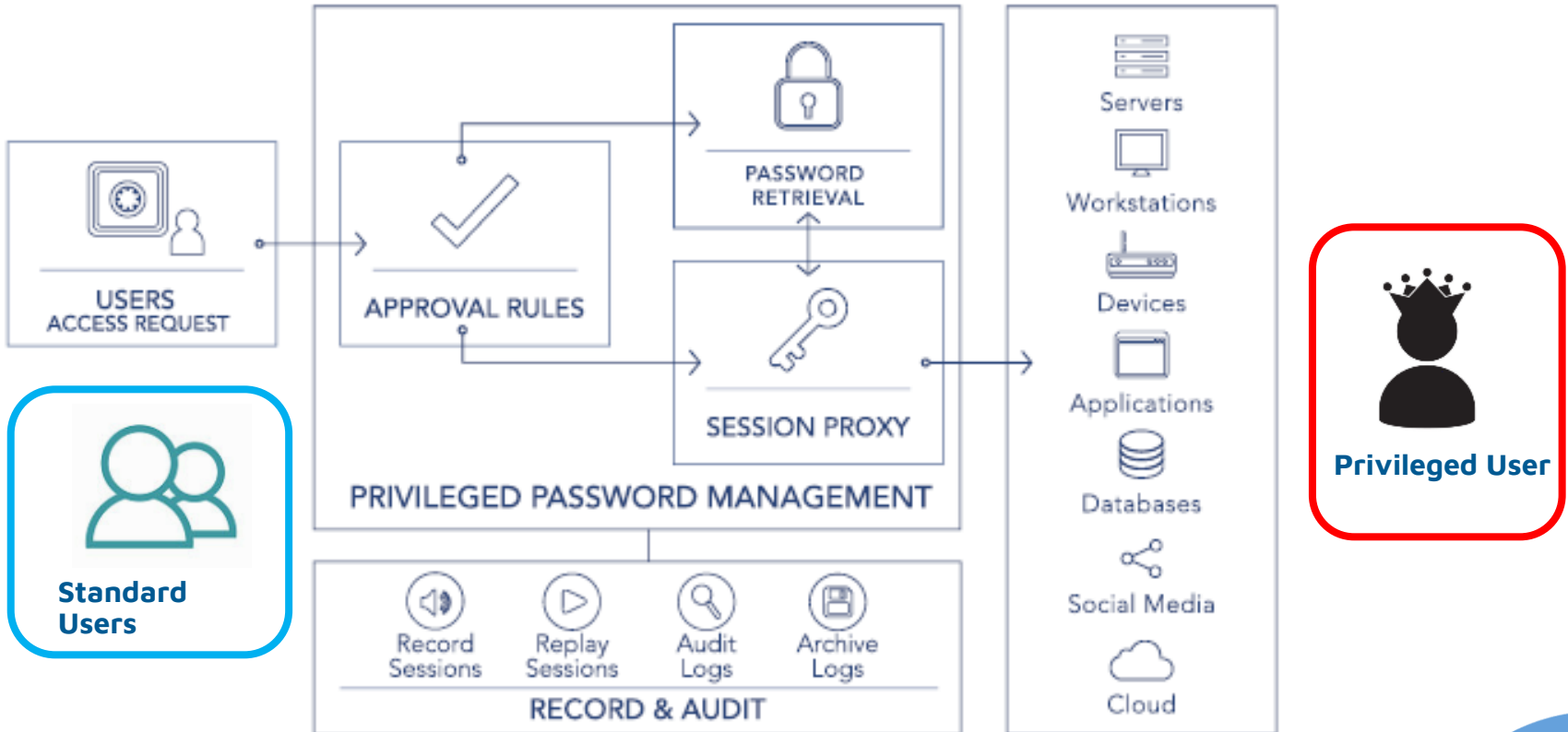
- Con un modello di sicurezza che fornisce l'accesso sensibile al contesto al server effettivo; in questo caso l'accesso RO al server effettivo in cui è in esecuzione l'istanza SQL e un'opzione per eseguire solo lo Microsoft SQL ManagementStudio con diritti elevati.

Come può aiutarti ManageEngine



Elevazione dei privilegi self-service con l'application control

Configura l'assegnazione dei privilegi self-service per determinati endpoint usando un approccio agent-based





Approccio a 6 step per ridurre i rischi legati agli accessi privilegiati

- 1. Conduci un audit completo su tutti gli account e i loro privilegi
- 2. Assegna i privilegi minimi predefiniti per gli account utente, che idealmente dovrebbero essere impostati sul grado più basso possibile
- 3. Implementa controlli sull'assegnazione dei privilegi just-in-time
- 4. Rimuovi privilegi amministrativi ingiustificati e in eccesso
- 5. Elimina l'hard-coding delle credenziali
- 6. Esegui il controllo delle applicazioni e dei comandi



- **Identifica ed elimina** i privilegi permanenti ed eccessivi
- **Revisiona** regolarmente i privilegi per identificare ed eventualmente correggere le incongruenze
- **Ruota** password, chiavi e Certificati TLS periodicamente
- Applica workflows per il controllo degli accessi basato su ruolo, tempo e requisiti per l'approvazione dell'accesso elevato
- **Registra e tieni sotto controllo** le attività privilegiate in tutta l'azienda
- **Implementa** la MFA per aggiungere un ulteriore livello di sicurezza

L'approccio Zero Trust al PAM di PAM360

- Approccio olistico allo Zero Trust per il PAM
- PAM360 racchiude i tre principi fondamentali del PAM in architettura Zero Trust:



Verificare sempre

- Fattori in tempo reale
- Controllo degli accessi per per gli utenti basato su criteri
- Autenticazione a più fattori



Accesso con privilegio minimo

- Fine-grained RBAC
- Richiesta workflows
- Elevazione privilegio just-in-time



Assume breach

- Punteggio di attendibilità del dispositivo in tempo reale per isolare i dispositivi sospetti
- Controllo degli accessi basato su policy relative agli endpoint
- Monitoraggio e shadowing della sessione remota
- Alert in tempo reale
- Audit e report completi

PAM360 una soluzione PAM unificata

Principali funzionalità ManageEngine PAM360

- Gestione degli account privilegiati (Password Manager)
- Gestione degli accessi privilegiati
- Gestione delle sessioni privilegiate
- Gestione chiavi SSL e SSH
- Automazione intelligente del flusso di lavoro



Privileged account management
Account discovery, vaulting & access governance



SSH key management



SSL / TLS certificate management



DevOps and cloud security



Just-in-time privilege elevation



Secure remote access provisioning



Privileged session monitoring



User behavior analytics



Comprehensive auditing and reporting

PAM360: Principali caratteristiche funzionali



Proteggere e gestire gli account privilegiati in modalità centralizzata, mediando l'utilizzo delle credenziali privilegiate sui sistemi target sulla base di policy predefinite



Isolare le sessioni degli utenti proteggendo i sistemi target, controllando e consentendo l'accesso in modalità privilegiata senza il bisogno di esporre le credenziali di accesso



Password Vault per una gestione e condivisione centralizzata e sicura delle credenziali



Registrazione video di tutte le sessioni in cui l'utente privilegiato interagisce con un target.

Il valore aggiunto di ManageEngine PAM360

Lo scopo principale è quello di dare evidenza non solo sul **“chi”** ma anche sul **“cosa”** sia esattamente accaduto durante le sessioni di lavoro, fornendo gli strumenti necessari per l'individuazione delle **fonti di prova** relative a eventuali attività dannose accidentali o volontarie, fughe di informazioni, ecc e per raccogliere il massimo numero di **evidenze** con le quali agevolare la successiva indagine.

THANK YOU!

***Grazie mille
per la vostra attenzione!***

THANK YOU!

