Privileged Identity and Access Management

Indice

- Tecniche di autenticazione e multi-factor authentication
- Protocolli di autenticazione
- Gestione delle password e dei certificati.
- Modelli e tecniche per autorizzazione e controllo dell’accesso
- Privileged Identity and Access Management (PAM)
- Cenni sulla segregazione e segmentazione delle reti

Indice

- Tecniche di autenticazione e multi-factor authentication
- Protocolli di autenticazione
- Gestione delle password e dei certificati.
- Modelli e tecniche per autorizzazione e controllo dell'accesso
- Privileged Identity and Access Management (PAM)
- Cenni sulla segregazione e segmentazione delle reti

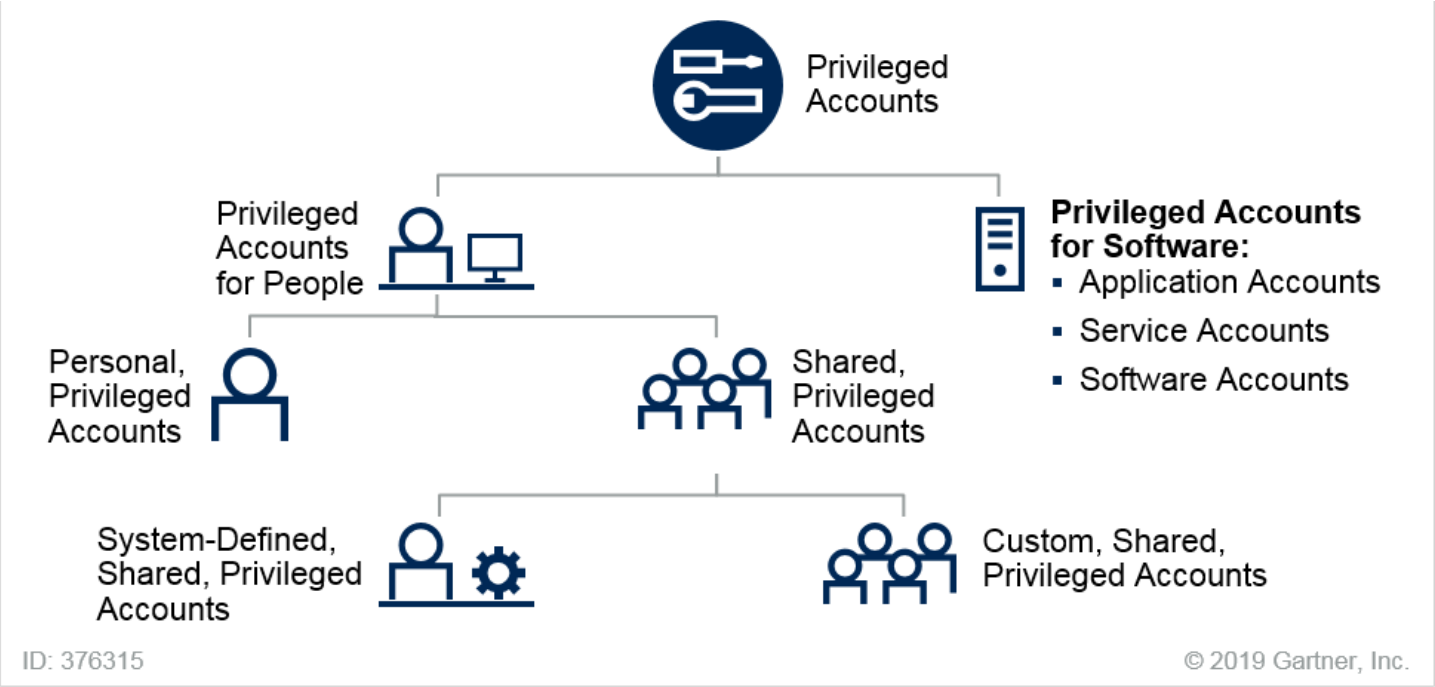
Privileged Identity and Access Management (PAM)

- L'accesso di *tutti* gli utenti di un sistema deve essere costantemente monitorato
  - Utenti sono sia persone, sia applicazioni
- La gestione e il controllo degli accessi da parte di utenze con privilegi elevati (PAM) è stato indicato come priorità da Gartner per il 2019

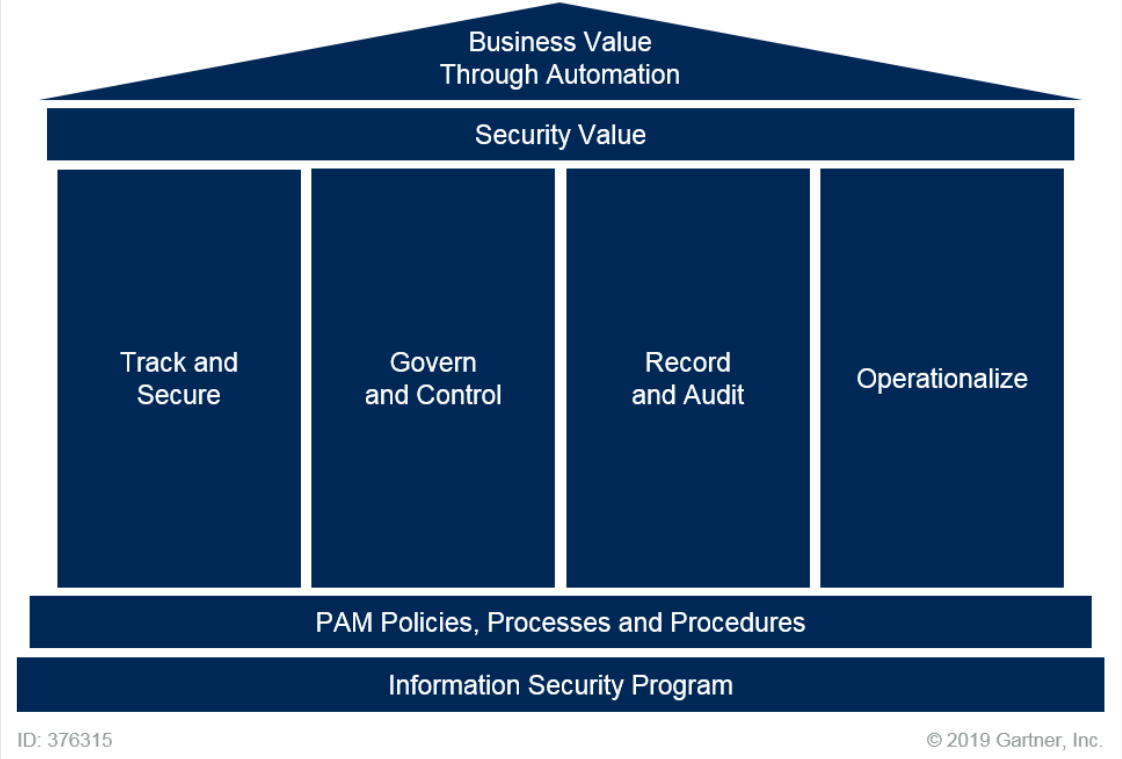
  https://www.gartner.com/en/documents/3899567/best-practices-for-privileged-access-management-through-

Tassonomia delle utenze privilegiate

da: Gartner, Best Practices for Privileged Access Management Through the Four Pillars of PAM, Gennaio 2019



PAM - I quattro pilastri secondo Gartner



da: Gartner, Best Practices for Privileged Access Management Through the Four Pillars of PAM, Gennaio 2019

Inventario delle utenze privilegiate

1. Individuare *tutte* le utenze privilegiate
2. Identificare *chi* utilizza le utenze privilegiate
3. Inventario dei *proprietari* di dati e di applicazioni che richiedono l'accesso da utenze privilegiate
4. Eliminare utenze *non necessarie* per razionalizzare gli accessi
   - Utilizzo di account condivisi da utenze con stesso ruolo

Inventario delle utenze privilegiate

1. Individuare *tutte* le utenze privilegiate
2. Identificare *chi* utilizza le utenze privilegiate
3. Inventario dei *proprietari* di dati e di applicazioni che richiedono l'accesso da utenze privilegiate
4. Eliminare utenze *non necessarie* per razionalizzare gli accessi
   - Utilizzo di account condivisi da utenze con stesso ruolo

Inventario delle utenze privilegiate

1. Individuare *tutte* le utenze privilegiate
2. Identificare *chi* utilizza le utenze privilegiate
3. Inventario dei *proprietari* di dati e di applicazioni che richiedono l'accesso da utenze privilegiate
4. Eliminare utenze *non necessarie* per razionalizzare gli accessi
   - Utilizzo di account condivisi da utenze con stesso ruolo

Inventario delle utenze privilegiate

1. Individuare *tutte* le utenze privilegiate
2. Identificare *chi* utilizza le utenze privilegiate
3. Inventario dei *proprietari* di dati e di applicazioni che richiedono l'accesso da utenze privilegiate
4. Eliminare utenze *non necessarie* per razionalizzare gli accessi
   - Utilizzo di account condivisi da utenze con stesso ruolo

Controllo degli accessi privilegiati

- JIT (Just-In-Time) access
  Evitare accessi persistenti ma autorizzare solo **accessi limitati nel tempo** e limitati **nelle capacità**
  - Automatico con strumenti PASM (privileged account and session management), o con approvazione da parte di persona responsabile
  - Accesso privilegiato anche da account non privilegiato con strumenti PEDM (privilege elevation and delegation management), analogo a ‘su’ e ‘sudo’ di UNIX/Linux

Controllo degli accessi privilegiati

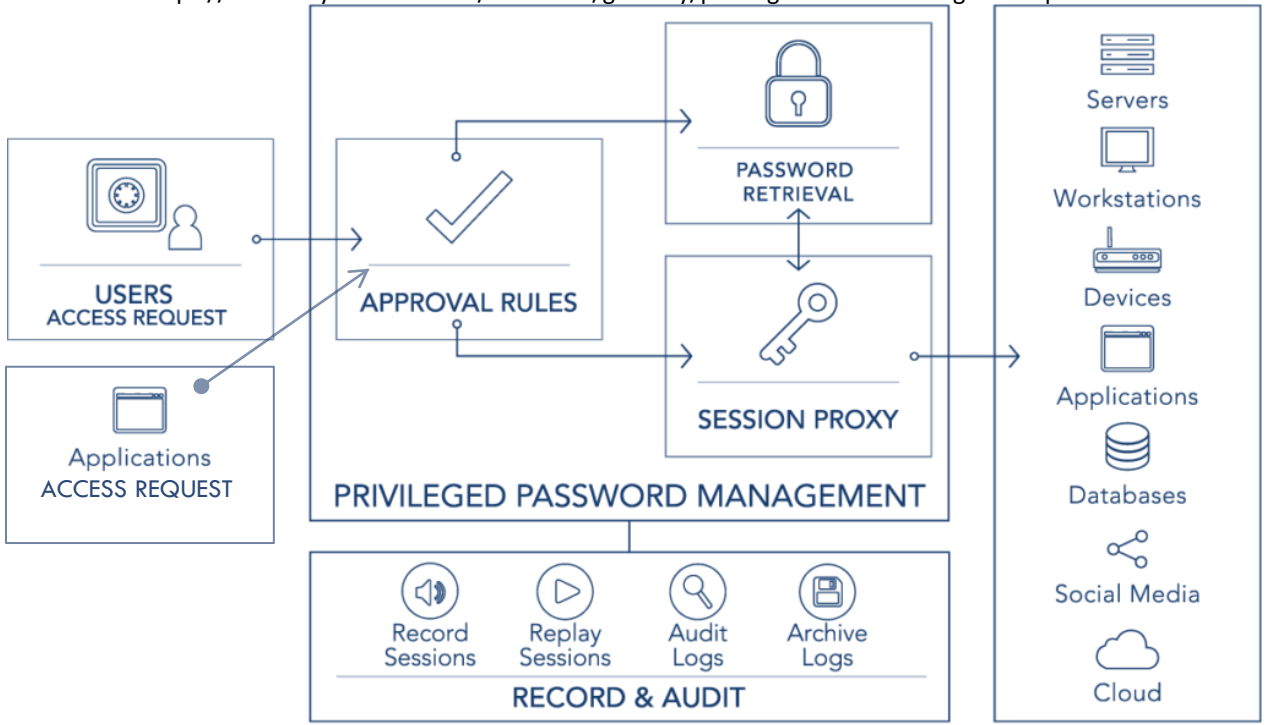
- JIT (Just-In-Time) access
  Evitare accessi persistenti ma autorizzare solo **accessi limitati nel tempo** e limitati **nelle capacità**
  - Automatico con strumenti PASM (privileged account and session management), o con approvazione da parte di persona responsabile
  - Accesso privilegiato anche da account non privilegiato con strumenti PEDM (privilege elevation and delegation management), analogo a ‘su’ e ‘sudo’ di UNIX/Linux

Controllo degli accessi privilegiati

- JIT (Just-In-Time) access
  Evitare accessi persistenti ma autorizzare solo **accessi limitati nel tempo** e limitati **nelle capacità**
  - Automatico con strumenti PASM (privileged account and session management), o con approvazione da parte di persona responsabile
  - Accesso privilegiato anche da account non privilegiato con strumenti PEDM (privilege elevation and delegation management), analogo a ‘su’ e ‘sudo’ di UNIX/Linux

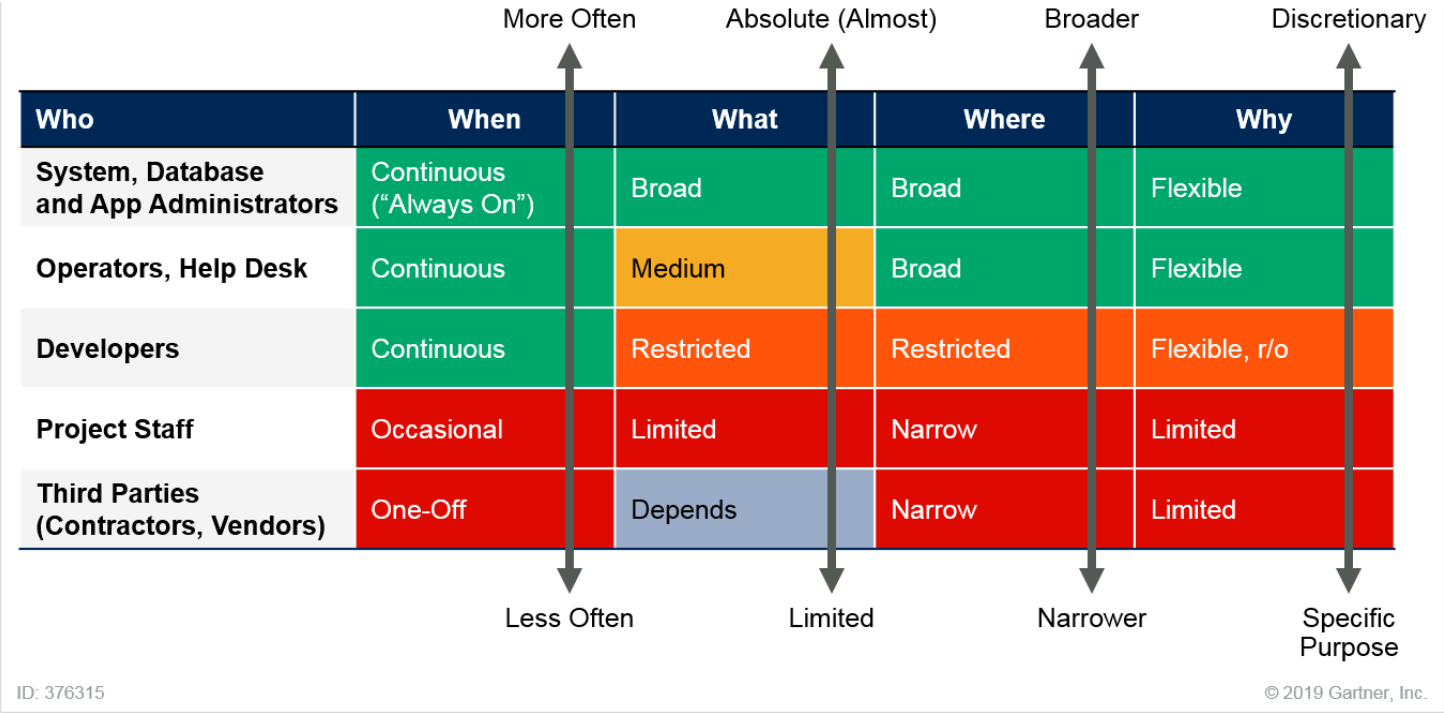
Implementazione di PAM

Adattamento da https://www.beyondtrust.com/resources/glossary/privileged-access-management-pam



Le cinque ’W’ degli accessi privilegiati

da: Gartner, Best Practices for Privileged Access Management Through the Four Pillars of PAM, Gennaio 2019



Monitoraggio degli accessi privilegiati

- File di log degli accessi e delle attività svolte
- Combinazione di più strumenti
  - Log dei database per accesso amministratori
  - Log di sistemi di monitoraggio modifiche di file
  - Log delle sessioni create da strumenti PAM
  - SIEM per UEBA (user event behavior analysis)