Preempt and Privileged Account Management

Preempt makes it easy to actively monitor, manage, and protect your most privileged users and accounts while simultaneously protecting all users and assets from risk and cyber threats.

In response to the risks posed by cyber attacks and breaches, many organizations are investing in additional security controls to more proactively manage their privileged users and accounts. Privileged Access Management (PAM) is a rapidly growing category of products that specifically targets this use case.

Although Preempt is not a purpose-built PAM solution, it is able to meet and exceed many of the core features of a PAM while bringing a wealth of additional capabilities that serve the larger goal of stopping attacks and reducing risk. As a result, Preempt can be either an alternative or a compliment to a PAM based on the particular needs and requirements of the environment. To this end, this document provides a brief introduction to Preempt's key capabilities with regard to privileged users, and the similarities and differences with traditional PAM solutions.

Preempt Key Features for Privileged Accounts

Privileged Account Discovery

Preempt automatically identifies all privileged users and accounts in the enterprise network including human as well as service accounts.

Device Tracking

Track and report on devices associated with privileged users based on observed activity. Allows staff to identify machines with administrator hashes and enforce appropriate controls over them.

Key Use Cases

+ **Risk Reduction** – Automatically track all privileged accounts and devices and take action on risky behavior or configurations such as weak passwords or use of unmanaged devices.
+ **Detect and Prevent the Use of Compromised Accounts** – Identify compromised accounts based on behavior or detection of malicious techniques and take automated protective action.
+ **Detect and Prevent Insider Access Abuse** – Control password sharing, shared accounts, or end-users using service account credentials.
+ **Safely Enable Staff** – Integrate multifactor authentication to any application to verify identity without reducing productivity.

Behavioral Monitoring

Automated, real-time baselining and anomaly detection of all privileged account behavior including time, location, assets accessed, protocols used and wide variety of account traits.

Adaptive Policy-Based Controls

Verify identity, trigger multi-factor authentication, reduce permissions, force password change, or block based on policy and context

Checks and Balances

Create human authorizers for service accounts or cross-authorizers between administrators.

Monitor and Enforce Password Hygiene

Track and enforce policy based on password strength and age. Find exposed passwords, shared passwords, or passwords that have been compromised in a previous breach.

Track Privileged User Risk

Identify and score risky behavior including shared accounts, shared devices, use of unmanaged devices, use of stale accounts, service account abuse, and more..

Going Beyond Privileged Account Management

Simple Deployment

Preempt provides a simple, centralized deployment that delivers value quickly and easily, and provides enforcement without the need of an agent on the protected devices.

Respond Appropriately

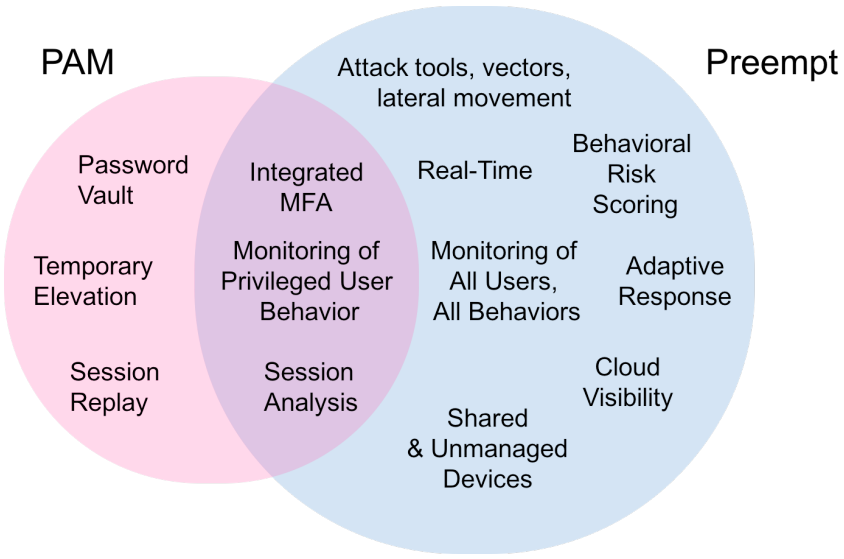
Flexible policy responses allows response to adaptively scale with the risk to avoid political challenges common in PAM deployments.

Superior CyberSecurity Depth and Breadth

Preempt identifies threats across the entire lifecycle of a cyberattack including reconnaissance, use of compromised credentials, attacks on internal infrastructure, and much more.

Protection for All Users and Accounts

Preempt is equally effective at controlling privileged service accounts and easily extends to the management of non-privileged users.



Preempt complements and extends traditional PAM solutions with a comprehensive cybersecurity platform that protects all users and accounts

www.Preempt.com

info@preempt.com

Preempt protects enterprises from security breaches and malicious insiders with an innovative and patented platform that couples User Behavior Analysis and Adaptive Response to provide the most effective solution for both detecting and automatically responding to security threats. This proactive approach allows organizations to preempt threats in real-time without engaging already overwhelmed security teams.