Going Beyond IAM with Identity and Access Threat Prevention

Preempt brings a new approach to enterprise security called Identity and Access Threat Prevention (IATP). As the name implies, this approach bridges the worlds of enterprise access and real-time threat prevention and policy enforcement. Much like Access Management (IAM) solutions, Preempt recognizes that user and account identity is one of the only reliable traits for enforcing policy as enterprises become increasingly unbound from the traditional perimeter and single-use devices. However, as has always been the case, simply managing access is not the same as security. Preempt and IATP introduces a truly new security layer that delivers enterprise-wide visibility of identity and access, reveals risks, enforces policy, and preempts threats based on identity, behavior, and risk.

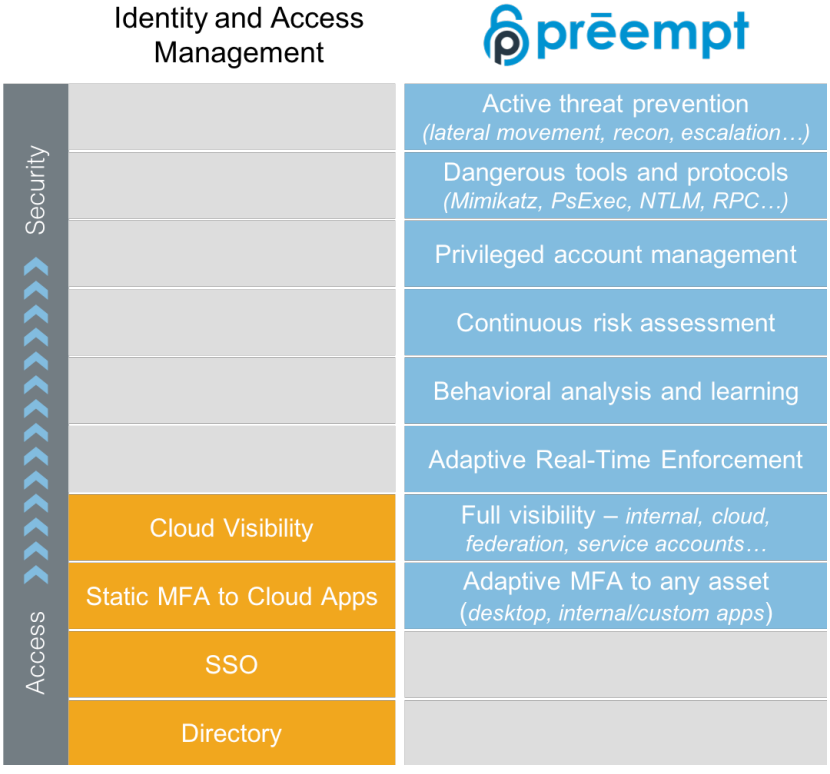
This approach naturally complements the functions of IAM, and often the approaches work hand-in-hand. This document highlights some of the key differences and capabilities of Preempt beyond that of a traditional IAM, and how they can be used together in a modern security architecture.

Detect and Block Active Attacks and Threats

Preempt analyzes network traffic as well as logs to identify a wide variety of malicious behaviors in the enterprise. This includes the detection of attackers performing reconnaissance, lateral movement, privilege escalation including techniques such as pass-the-hash, Golden Ticket, and relay attacks.

Control Over Dangerous Tools and Protocols

In addition to stopping malicious techniques, Preempt also provides real-time control over a variety of high-risk tools and protocols. For example, Preempt can detect and block tools such as Mimikatz, which has become a staple of an attacker's arsenal. Preempt can also provide contextual control over tools and protocols such as PsExec, NTLM, or RPC, which can have valid uses, but can cause problems if abused by attackers.



Holistic View of Identity and Access

Preempt acts as a proxy to the authentication infrastructure and directly monitors network traffic as well as AD logs to track all user and account behavior. The solution easily integrates with SSO and federation services to ensure an authoritative view of "who is using what" across the entire enterprise.

Behavioral Monitoring and Access Control

Preempt continually monitors and learns the behavior of all accounts inside the network including the applications, services, protocols, devices and normal hours and location for a given account. Preempt can challenge suspicious behavior before access is granted. If validated, the event is automatically closed and the result fed back into the Preempt solution to further train the machine learning models.

Policy-Based Adaptive Enforcement

Preempt offers a wide range of policy-based responses to that align to the observed level of risk. This includes blocking, MFA, reduction of user privileges, force password change, require an authorizer, or isolate the user from the Internet. All responses can be adaptively triggered based on identity, behavior, risk level, and other enterprise and event contexts.

Management of Privileged Accounts

Preempt monitors all accounts in the enterprise and directly analyzes traffic to automatically identify privileged accounts including all service accounts in the network. Preempt analyzes actual permissions to identify "stealthy administrators", continually monitors all privileged accounts for weaknesses, and allows both manual and automated policies to manage privileged accounts.

Desktop MFA and Control Over Any Asset

Preempt enforces fine-grained adaptive access policies for any asset in the enterprise including the ability to extend adaptive MFA to individual workstations, servers or to remote logins. Preempt can likewise add adaptive MFA to any internal application including custom or legacy applications without requiring custom coding to the application itself.

Continuous Audit and Risk Scoring

Preempt constantly audits all users and accounts for problems and scores them in terms of risk to the enterprise. Risk scores can be driven based on a wide variety of factors including password strength, the use of unmanaged devices, changes in behavior, sharing of devices or passwords, as well as the privileges of the account including any stealthy administration privileges.

Proactive Threat Hunting

In addition to real-time enforcement, Preempt provides a platform for analysts to actively hunt for threats. Analysts can easily search across any attribute tracked by the Preempt Platform, to find low-level signs of an attack and see events in chronological context.

Detailed Reporting

Preempt not only protects the environment, but also provides documentation and reporting to share with the organization and support compliance efforts. Reports can be created for virtually any Preempt information such as security incidents, observed anomalies, device reports, dangerous protocols, privileged users and much more. Reports can be run manually or scheduled to be run and delivered at automated intervals.

Better Together

As discussed above, Preempt naturally integrates with an IAM's MFA capabilities to deliver a new highly-flexible approach to MFA that adapts in response to changes in context and risk. Preempt also integrates with the IAM's SSO capabilities to extend and unify visibility between the internal network and the cloud. By integrating the two solutions, organizations ensure full visibility across the entire enterprise, while delivering the ability to find and stop threats with the right control at the right time.

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.