Identity & Access Threat Prevention

Continuously preempt threats based on identity, behavior and risk with the Preempt Platform

As enterprises transition to the cloud and the perimeter disappears, identity is the new perimeter. To preempt threats and breaches, the identity teams and security teams must come together to approach the problem in a new, continuous, adaptive and preemptive way with Identity and Access Threat Prevention. And without a holistic view of all users, privileges, access patterns and accounts, having proper controls over accounts can be difficult. This is where we are changing the game and the Preempt Platform delivers.

Core Values for Customers

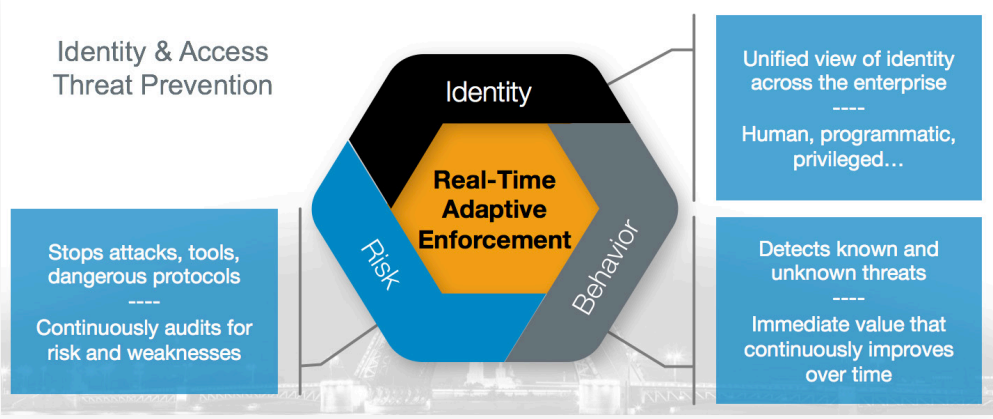
+ **Preempt Security Incidents and Threats**
+ **Unify Visibility of Accounts Across All Platforms**
+ **Increase Efficiency of Security Operations**

The Preempt Platform

With the Preempt Platform, organizations can automatically respond in real-time to anomalous or risky behavior, proactively add secure access control and resolve risk and weaknesses before they are exploited by attackers. Uniquely, the Platform uses identity, behavior and risk to continuously and situationally adapt to ensure the right level of security at the right time across all resources (on prem, cloud and hybrid).

The Platform offers a core set of capabilities and applications that support a broad variety of use cases. The flexibility of the Platform allows customers to implement Identity and Access Threat Prevention at a pace and scale that works best in their environment and on any network resource where secure access is required.

.



Core Platform Capabilities

The Preempt Platform has several core capabilities. These include:

Real-time Adaptive Response

Real-time adaptive response stops threats without getting an analyst involved or disrupting valid user behavior. Preempt offers a variety of policy-based responses (e.g. Block, MFA, Isolation, reduce privileges, alert, etc) and can continually adapt based on identity, behavior and risk. For example, a potentially compromised privileged user could be challenged with MFA to verify identity. When a threat is confirmed, the user can be blocked, isolated or demoted.

Unified and Continuous Visibility

Gain visibility into who is accessing what, when, where and how. All user activity can be seen in one place including access, behavior, history, profile changes, locations, device, role, password strength, privileges, VPN, SSO, authentication requests and more. Preempt analyzes real-time traffic and logs to understand behavior and reveal risks (stealthy admins, hidden objects, exposed passwords, weak passwords, stale users, privileged users, etc.). Visibility allows for better controlling privileged accounts, responding to incidents, more efficient audits and more.

Tool and Protocol Containment

Preempt's unique detection capabilities allow enterprises to prevent lateral movement and unauthorized domain access due to the misuse of network tools (eg. PsExec, PowerShell) and the use of hacking tools (eg. Mimikatz, etc). Preempt also has the ability to deeply inspect authentication protocols (NTLM, Kerberos, LDAP) to help control protocol usage and reduce risk of credential forwarding and password cracking as well as detecting attacks like Pass-the-Hash and Golden Ticket.

Context Based Access Controls

Preempt can provide immediate protection of internal resources by either setting up policy based enforcement or easily adding any MFA in front of any network resources without the need for doing development. Organizations can determine and enforce who is able to access what resource and in what context (eg. role, device, location, etc.). For example, restricting access to sensitive servers by contractors, interactive logins by service accounts, privileged account usage, etc.

Extensible Integrations

With an open and extensible architecture, Preempt delivers consistent security and user experience across on prem, cloud or hybrid environments. With a broad set of integrations, organizations gain more value out of security investments that have already been made and gain more intelligence for greater context and enforcement.

Platform Applications

Behavioral Firewall

The Behavioral Firewall provides real-time adaptive enforcement. It's goal is to detect, challenge and respond to threats and risky behavior without getting a security analyst involved. When an anomaly or risky behavior is detected, the Behavioral Firewall will challenge the suspicious behavior by proactively engaging with users to verify identity, get definitive answers and enforce policy. The solution automatically acts in proportion to risk.

Any App

Any App allows organizations to quickly and easily expand secure authentication to any network resource without having to do any additional development. Any App takes advantage of the Platform's highly-adaptable policy engine and easily takes on the role of an authentication and application proxy to prevent credential compromise. Preempt is vendor neutral and can extend a typical MFA deployment from a variety of vendors.

Insights

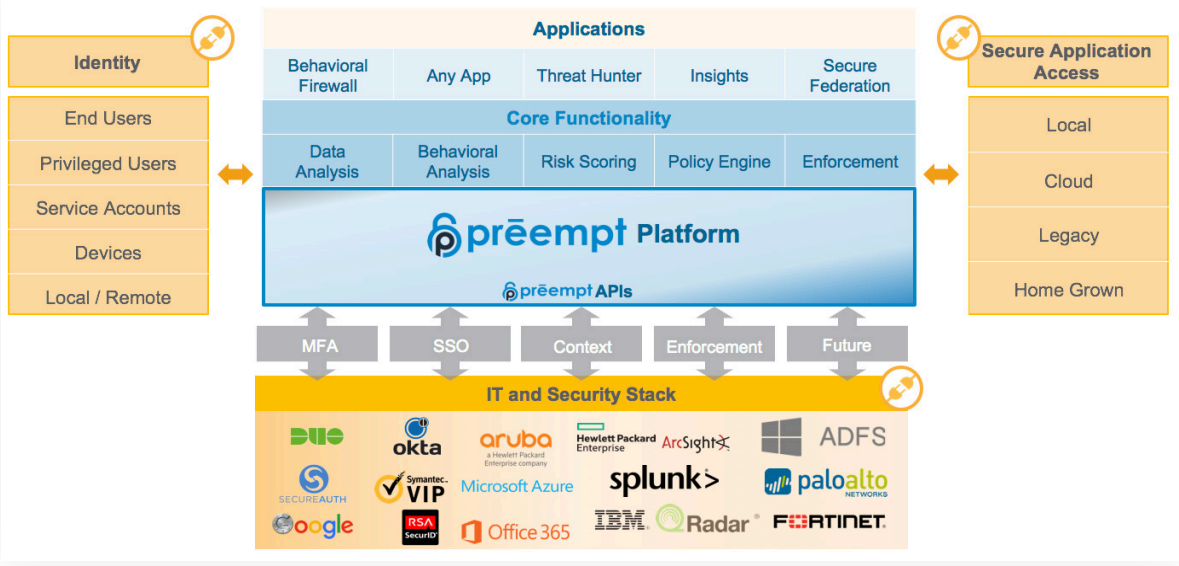
The Insights application provides a holistic view of identity and instant visibility into your security posture so you can proactively resolve risks and weaknesses before they are exploited by attackers. Quickly find privileged accounts you didn't know about, the use of shared accounts, and track use of unmanaged devices, weak or exposed passwords, or passwords that never expire.

Threat Hunter

Threat Hunter allows security analysts to proactively search through raw events, detect and identify security events or further investigate reported security events. It can also be used to find and eliminate threats such as administrative account lockouts, privilege escalation and failed logins. It provides a broad array of search criteria such as time/date, domain, site geo location, user and endpoint parameter, authentication events, service access account related events and more.

Secure Federation

Secure Federation provides adaptive identity verification and conditional controls to federated services (such as Active Directory Federation Services (ADFS) enabled applications like Office 365) via web browser or desktop applications. This also includes additional applications that are configured for SSO via ADFS federation.



How Customers Use The Preempt Platform

Eliminate Breaches and Compromised Credentials

+ Compromised accounts/ devices
+ Lateral movement
+ Infrastructure attacks
+ Unauthorized 3rd Party vendor access

Prevent Insider Threats

+ Malicious behavior
+ Abuse of privileges
+ Restricted data access
+ Risky or careless behavior

Manage and Protect Privileged Accounts

+ Privileged account discovery
+ Risk assessment of privileged user
+ Business privilege monitoring
+ Privileged identity use

Easily Add Identity Based Access Controls

+ Workstation login identity verification
+ High value servers and application access
+ Access based on policy
+ Add MFA to any application

Improve Incident Response and Forensics Efficiency

+ Automated reduction of alerts
+ Event triage and prioritization
+ Forensic and behavior chronology analysis

Reduce Risk and Support Compliance

+ Unaccessed servers and stale account mitigation
+ Weak, shared, exposed password identification and reset automation
+ Audit and compliance reports

Immediate Value

Not only does it take minimal time and effort to install and maintain the Preempt Platform but once installed you can immediately reduce attack surface and gain protection from deterministic attacks and internal threats.

Industry Leading Research

Preempt's dedicated security research team is constantly working to stay ahead of emerging risks. Their deep expertises of authorization and authentication protocols has helped them identify several critical Microsoft vulnerabilities and the team has been recognized and by the cyber industry as an innovative thought leader.

> ***"We looked at least four other solutions and none of the other solutions allowed us to be able to block and respond to threats in real-time. This was the driving factor for us selecting Preempt."***
>
> CISO at large Insurance association

www.Preempt.com

info@preempt.com

Preempt protects organizations by eliminating internal threats and security breaches. Threats are not black or white and the Preempt Platform is the only solution that delivers identity and access threat prevention that continuously preempts threats based on identity, behavior and risk. This ensures that both security threats and risky employee activities are responded to with the right level of security at the right time.