Secure Enterprises and Preempt Threats with Conditional Access

If you struggle with identifying all of the users and accounts in your organization, as well understanding what they are doing and accessing, it can be very difficult to be proactive at reducing risk and preventing threats. The Preempt Platform takes a modern approach to authentication and securing identity and helps put you back in the driver’s seat so you can reduce risk and automatically preempt threats before they impact your business.

A New Approach To Threat Prevention

The Platform quickly discovers all of the users in your network and delivers continuous risk insights and behavioral analytics to better detect and respond to threats in real-time before they impact your business. The unique adaptive capabilities of the Platform allow you to automate threat response with the right type of enforcement or notification based on identity, behavior and risk. This ensures the right level of security is delivered to either stop a threat or allow valid users to get on with their work.

Preempt adapts with your organization as it grows and changes, whether it be on-premises or in the cloud. You can get started with the benefits of the Preempt Platform in as little as two hours and gain immediate and ongoing benefits.
THE PREEMPT PLATFORM

Platform Components

Identity and Risk Insights

Organizations often have siloed or incomplete views of who is accessing what, when, where and how across multiple security solutions and platforms. Preempt solves this by auto-discovering and continuously monitoring all users, privileges, accounts and access whether on premises or in the cloud.

With a single easy to use management console, Identity and Risk Insights provides a continuous health and risk assessment – revealing password problems, privileged access, stealthy admins, Active Directory (AD) configuration issues and more so that you can gain more control over all accounts (users, privileged, service and more) while at the same time allowing your security team to easily and proactively reduce risk and the attack surface, making it easier to pass your next audit.

Analytics and Threat Detection

The Platform’s User and Entity Behavior Analytics learns the behavior of every user and device on the network, including privileged users and service accounts, and develops risk scoring for each of them. The system classifies users and machines and measures risk based on a variety of factors including activity from Cloud services, SSO, VPN, supervised and unsupervised learning and real-time authentication traffic.

Analytics can expose risky user behavior, malicious insiders, attackers, compromised accounts or devices, lateral movement, attempts to escalate privileges, and attacks against internal infrastructure.

Credential based attacks continue to be the number one way organizations are compromised. Preempt approaches threat detection differently. By combining analytics that are focused on identity, behavior and risk with real time traffic (either passive/sniffer mode or inline), you gain greater fidelity in attack detection.

Lose the silos and reduce risk with unified visibility

- Continuously discover all users: privileged, service accounts, regular users, stale accounts
- Develop unified user access profiles and identify suspicious behavior
- Reduce risk and find problems before attackers do

Uniquely, with the Preempt Platform, you can prevent lateral movement and unauthorized domain access due to the misuse of network tools (e.g. PsExec, PowerShell) and the use of hacking tools (e.g. Mimikatz, Bloodhound, etc). Preempt also has the ability to deeply inspect authentication protocols (NTLM, Kerberos, LDAP, etc) to help control insecure protocol usage and reduce risk of security threats, including credential forwarding and password cracking as well as detecting attacks like Kerberoasting, Pass-the-Hash and Golden Ticket.

Detect & investigate credential based threats in real-time

- Real-time detection of suspicious or risky behavior
- Identification of deterministic attacks and use of malicious attack tools
- Enhanced investigations and threat hunting
- Identify areas of risk that can be better controlled with Conditional Access
Conditional Access for Threat Prevention

When you have a team overwhelmed with security incidents, it becomes impossible to respond to every threat. Now when suspicious behavior is detected, the Platform’s conditional access capabilities can step in to help proactively respond to threats without getting an analyst involved or disrupting valid users.

Preempt can progressively interact with users to verify threats and enforce policy. Fine-grained actions allow you to match the level of response to the risk, and can automatically adapt based on changing context.

Policy-based responses (e.g. Block, MFA, Isolation, reduce privileges, alert, allow, etc.) continually adapt based on identity, behavior and risk. For example: an MFA challenge can be pushed to a user based on risky behavior before granting access.

Adaptive MFA provides the ultimate flexibility based on your needs and policies:
- Gain immediate protection of internal resources by adding policy based enforcement
- Easily add MFA in front of any network resource without modifying the application or adding endpoint agents
- Determine and enforce who is able to access what resource and in what context (e.g. role, device, location, etc.)

Example: restrict access to sensitive servers by contractors, interactive logins by service accounts and more

Preempt Threats Before Impact

- Stop threats in real-time
- Maximize efficiency with automated response
- Add conditional access for on prem or cloud apps
- Add MFA to any resource without development and with no endpoint agents

Contextual Data Sources:
Network Traffic/Logs/Third Party Integrations

Enforcement Options:
Adaptive MFA/Reduce Privileges/Quarantine, Block, + more
Preempt delivers a modern approach to authentication and securing identity with the market’s first solution to deliver Conditional Access for continuously detecting and preempting threats based on identity, behavior and risk. Preempt’s patented technology empowers Enterprises to optimize Identity hygiene and stop attackers and insider threats in real-time before they impact business.

## How Customers Use the Preempt Platform

### Adaptive MFA
- Conditional Access based on identity, behavior and risk
- Workstation login identity verification
- High value servers and application access
- Access based on policy
- Add MFA to any application
- Cloud, On Premises, Hybrid

### Privileged Account Security
- Privileged account discovery/use
- Risk assessment of privileged users
- Prevent privilege escalation, lateral movement
- Privilege access abuse
- Presence of stealthy (shadow) administrators
- Policy-based control

### Detect Insider Threats + Credential Compromise
- Compromised accounts/devices
- Lateral movement
- Infrastructure attacks like Golden Ticket or Kerberoasting
- Anomalous or risky behavior
- Restricted data access
- Spread of ransomware/malware

### Active Directory Security
- Workstation login identity verification
- High value servers and application access
- Access based on policy
- Add MFA to any application

### Value at Every Step

<table>
<thead>
<tr>
<th>Preempt Platform</th>
<th>Identity &amp; Risk Insights</th>
<th>Analytics &amp; Threat Detection</th>
<th>Conditional Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>User and Account Access Visibility</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>Discovery of Privileged Accounts</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>Discovery of Stealthy Admins &amp; Service Accounts</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>Password Health Visibility</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>Compliance &amp; Reporting</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>Risky User Behavior &amp; Anomaly Detection</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>Attack Tools &amp; Misuse of Protocols</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>Lateral Movement &amp; Threat Hunting</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>Adaptive Response and Policy Enforcement</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>Secure Federated Access to Cloud Apps</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>Secure Access Control for Any App</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
<tr>
<td>Real-Time Threat Prevention</td>
<td>☑️</td>
<td>☑️</td>
<td>☑️</td>
</tr>
</tbody>
</table>

“"We looked at four other solutions and no other product allowed us to be able to block and respond to threats in real-time.”

CISO AT LARGE INSURANCE ASSOCIATION