# The Preempt Platform

## Continuously reduce risk and preempt threats based on identity, behavior and risk

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 preventing threats. The Preempt Platform takes a new modern approach to the problem and helps put you back in the driver's seat so you can reduce risk and automatically preempt threats before they impact your business.

### Benefits

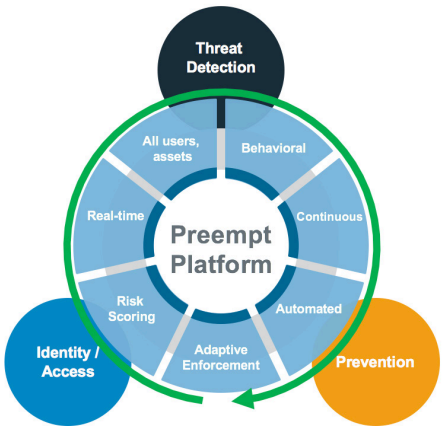
+ **Preempt Security Incidents and Threats**
+ **Continuous Unified Visibility of All Users Across the Enterprise**
+ **Increase Security Operations Efficiency**

## The Preempt Platform

The Platform quickly discovers all of the users in your network and delivers continuous insights and behavioral analytics to better detect and respond to risk and threats in real-time before they impact your business. And because threats are not black or white and can vary greatly, we help you take it a step further. The unique adaptive capabilities of the Platform allow you to automate 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.

We realize enterprise security infrastructures are not one size fits all. Our Platform supports teams of all sizes and maturity levels. As you get started on your journey to real-time threat prevention, Preempt adapts with your organization as it grows and changes, whether it be on premises or in the cloud. Best of all, you can get started with the benefits of the Preempt Platform in as little as two hours and gain immediate and ongoing benefits.

- **GAIN VISIBILITY** Into Identity, Behavior, and Risk of all Users and Accounts
- **DETECT** Threats Continuously
- **AUTOMATE RESPONSES** to Risk in Real-Time to Allow Valid Activity or Preempt Threats



# Platform Components

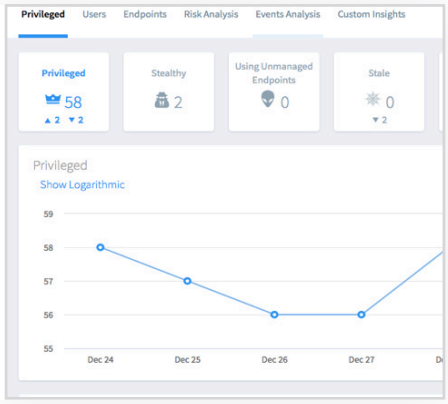
## Insights and Analytics

### What if you could get rid of the silos and reduce your risk on day one?

+ 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

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 all users, privileges, accounts and behavioral access patterns whether on premises, in the cloud, or in hybrid environments.

With a single easy to use management console, Insights and Analytics 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 the security team to easily and proactively reduce attack surface risk making it easier to pass your next audit.




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 network 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.

## Real-Time Threat Detection

### What if you could detect or 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

Credential based attacks continue to be the number one way organizations are compromised. Preempt approaches threat detection differently. By using Insights and Analytics that are focused on identity, behavior and risk with real-time network traffic, the Platform not only provides you with greater fidelity in attack detection but also reduces the amount of false positives that need to be managed and allows you to be more proactive in preventing threats and speeding up investigations.

Uniquely, with the Preempt Platform, you can 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, 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.

## Adaptive Threat Prevention

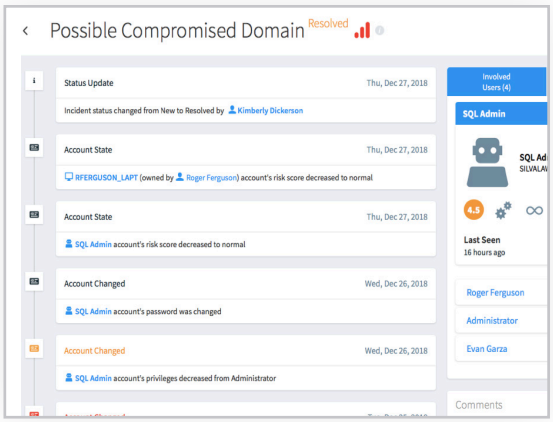
When you have a team overwhelmed with security events and incidents, it becomes impossible to respond to every threat in a timely manner. Now when suspicious or risky behavior is detected, the Platform's adaptive threat prevention capabilities can step in to help you proactively respond to threats without getting an analyst involved or disrupting valid users.

### What if you could preempt threats before impact?

- + Stop threats in real-time
- + Maximize efficiency with automated response
- + Add conditional access for on-prem and cloud apps
- + Add MFA to any resource without development

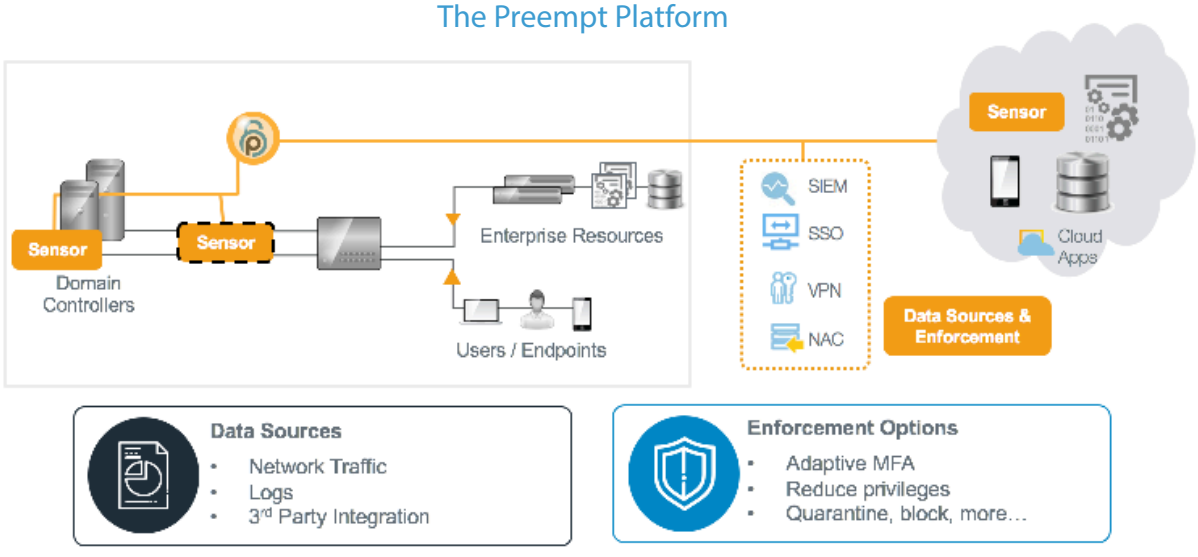
Preempt can progressively interact with users to verify threats and enforce policy. Fine-grained actions allow you to match the level of response to the risk, and can automatically adapt based on changing context.

Policy-based responses (e.g. Block, multi-factor authentication (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 suspicious behavior. If user fails the challenge, they can be blocked.




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

### The Preempt Platform



## How Customers Use The Preempt Platform

### Eliminate Breaches + Compromised Credentials

+ Compromised accounts/devices
+ Lateral movement
+ Infrastructure attacks like Golden Ticket or Kerberoasting
+ Spread of ransomware/malware across the enterprise

### Prevent Insider Threats

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

### Manage and Protect Privileged Accounts

+ Privileged account discovery and use
+ Risk assessment of privileged users
+ Prevent privilege escalation

### 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

## Value at Every Step

| | Preempt Platform | | |
|---|---|---|---|
| | **Insights and Analytics** | **Real-Time Threat Detection** | **Adaptive Threat Prevention** |
| User and Account Access Visibility | ✓ | ✓ | ✓ |
| Discovery of Privileged Accounts | ✓ | ✓ | ✓ |
| Discovery of Stealthy Admins & Service Accounts | ✓ | ✓ | ✓ |
| Password Health Visibility | ✓ | ✓ | ✓ |
| Compliance & Reporting | ✓ | ✓ | ✓ |
| Risky User Behavior & Anomaly Detection | | ✓ | ✓ |
| Attack Tools & Misuse of Protocols | | ✓ | ✓ |
| Lateral Movement & Threat Hunting | | ✓ | ✓ |
| Adaptive Response and Policy Enforcement | | | ✓ |
| Secure Federated Access to Cloud Apps | | | ✓ |
| Secure Access Control for Any App | | | ✓ |
| **Real-Time Threat Prevention** | | | ✓ |

*"We looked at least four other solutions and no other product 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.