The Preempt Behavioral Firewall scores the risk of every user, account, and device in the network, then delivers adaptive actions to verify and eliminate threats—all without manual intervention from your security team.

Capabilities

**User and Entity Behavior Analytics (UEBA)**
The Behavioral Firewall learns the behavior of every user and device on the network including privileged users and service accounts. The system exposes behavior of careless users, malicious insiders, and attackers such as compromised accounts or devices, lateral movement, attempts to escalate privileges, and attacks against internal infrastructure.

**Proactive Risk Scoring**
Every entity in the network is continuously scored in the context of role, observed behavior, and potential impact to assets. Scores adapt automatically in response to policy-based challenges such as multi-factor authentication, and are prioritized based on attributes such as a user’s privileges, role, password strength, peer group, associated endpoints, value of assets and multiple additional dimensions.

**Adaptive Response and Enforcement**
Based on policy, Preempt can progressively interact with suspicious users to verify threats and enforce policy without impacting valid users. For example, a potentially compromised user could be challenged with multi-factor authentication to verify identity. Users with weak passwords could be forced to change their password. When a threat is confirmed, the user can be blocked, isolated or demoted.

Preempt Behavioral Firewall
Turn behavioral analytics into real-time action that stops security breaches and insider threats without impacting your business

The real-time, automated, and appropriate threat enforcement includes:

- **Detect Hackers & Insider Threats:**
  Find attackers, insider threats, and risky behavior

- **Challenge Suspicious Behavior:**
  Proactively engage users to verify identity, get definitive answers, and enforce policy

- **Respond Appropriately:**
  Automatically act in proportion to the risk
Predictive Insights into the Attack Surface
Instant visibility into your security posture enables you to 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.

Use Cases
Security teams struggle to find practical approaches to dealing with threats without disrupting their business or overloading analysts. Despite promises, traditional UEBA tend to generate many false positives and require manual investigation. On the other hand, enforcement methods such as a next-generation firewalls lack an understanding of user behavior, and simple Allow or Deny responses risk disrupting the business.

The Behavioral Firewall bridges these two perspectives by pairing user behavior to detect threats with a contextual automated response that redirects risky user behavior and proactively stop threats without disrupting the business. Policies take into account a user or entity’s role, behavior, and the target of their actions. Flexible response options can redirect user behavior, confirm a threat, or block once a threat is verified. This provides enormous flexibility, which lends itself to a wide variety of use cases.

Active Threat Prevention

Compromised Accounts or Devices
Find signs that attackers or malware have compromised credentials or devices. Automatically challenge to verify user identity or block.

Lateral movement
Find a wide variety of lateral movement techniques such as Pass-the-Hash and attempts to escalate privileges.

Insider Access Abuse
Learn normal working hours, locations, and typical assets and applications to identify and challenge any anomalous behavior for detection of malicious insiders, naive users and those bending the rules to get things done.

Attacks against infrastructure
Find brute-force attacks, Golden Ticket attacks, forged PAC files, or attempts to harvest data from Active Directory.
Preempt Behavioral Firewall

**Increased Operational Efficiency**

**Event Triage and Prioritization**
Automatically prioritize based on a user’s privileges, assets accessed, observed behaviors, and any failed challenges. Automatically pinpoint the users posing the greatest risk to your business.

**Incident Response**
Accelerate times to detection and response. Automatically detect an incident, confirm any suspicious users or devices, and isolate them to prevent damage.

**Forensic Analysis**
Gain quick, meaningful insight into the behavior of any user, account, or device. Analysts can dig into a full chronology of the entity’s behavior with insight into how behavior deviated from previous norms.

**Visibility and Management of Risky Behavior**

**Privileged Users**
Automatically find all privileged users and accounts. Identify any unneeded stale privileged accounts, and monitor active accounts for suspicious behavior.

**Weak or Exposed Passwords**
Detect the use of weak passwords in the network to pinpoint insecure users and optionally force the user to reauthenticate and or change password based on policy.

**Shared accounts**
Quickly identify users or devices that are sharing accounts within the network and challenge to verify user identity.

**Monitor important users and assets**
Easily monitor and prioritize high-value users or assets such as executives or sensitive servers and databases.
Components

**Policy Engine**
The Policy Engine allows you to design policies that are both enforceable and appropriate to your business. Fine-grained actions allow you to match the level of response to the risk, and can automatically adapt based on changing context, ensuring risks are mitigated while the organization remains productive.

**Centralized Management**
Centralized management ensures Preempt can be deployed in any organization while retaining full visibility and control across all sites and locations. Staff can easily view Insights, incidents, statistics and maintain a coordinated workflow across the entire organization.

**Extensible Integrations**
Extensible integrations extend the value of your existing investments and provide additional perspectives of the network and empower Preempt’s Policy Engine with additional response options. The solution integrates with a variety of data intelligence providers, cloud single sign-on solutions, VPN concentrators, gateways, SIEMs, and enforcement solutions.

**Flexible Deployment**
The Preempt Behavioral Firewall can be deployed in either in-line or span port (sniffer) mode. The unique design enables threat response capabilities in both modes, ensuring that your security administrators only follow up on valid threats.

Preempt protects enterprises from security breaches, malicious insiders and risky behavior from naive users with an innovative and patented Behavioral Firewall that couples User and Entity Behavior Analytics and Adaptive Response to provide the most effective solution for preventing security threats. This proactive approach allows organizations to preempt threats in real-time without engaging already overwhelmed security teams.