preēmpt

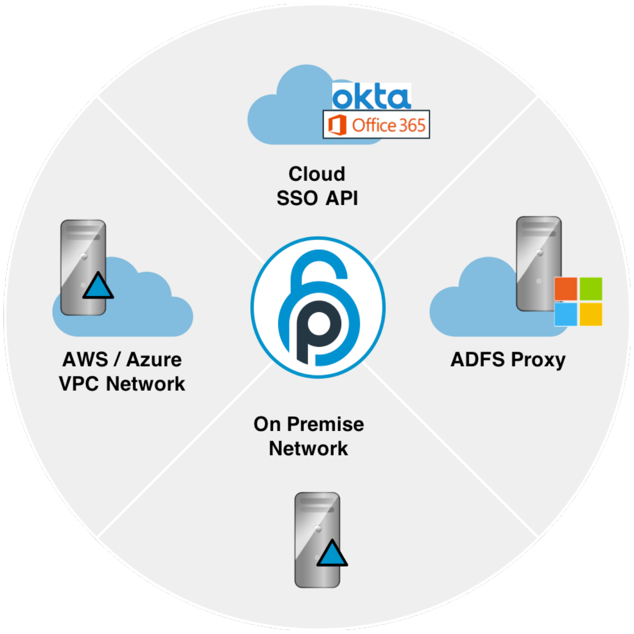
PRODUCT BRIEF

Preempt Secure Federated Access

Transition To The Cloud Without Risks or Weaknesses

The Preempt Secure Federated Access App ensures comprehensive and consistent visibility and enforcement that extends across all enterprise cloud-based assets. As organizations move to the cloud, it is common for security to become fractured and inconsistent compared to on-premise controls, which can open up new and unknown risks. The organization may have strong policies inside the traditional perimeter, but it is often hard for organizations to know who is accessing what in the cloud. Preempt's Secure Federated Access delivers a new approach to security that grows along with the enterprise so that security can easily see behavior of all identities, and make smart, adaptive enforcement decisions based on risk and complete enterprise context.

Preempt and Microsoft ADFS



Preempt integrates with Microsoft's Active Directory Federation Services (ADFS) as an authentication provider. At its most basic level this integration allows Preempt to extend visibility and control to the federated cloud applications, including Office 365, SalesForce, Workday, and others.

However this integration also allows organizations to extend a wide range of adaptive threat prevention and policy enforcement to these applications that was never possible before. For example, in the past if an organization wanted to include MFA for federated applications, the user would be challenged upon every application access.

With Preempt, the decision to challenge a user can be triggered based on situational policy, against observed risks and behavior. For example, MFA could only be required on a first access, or alternately based on the user's device, change in observed behavior, or a risky configuration.

Seamless Security to the Cloud

Preempt ensures that security grows right along with your investments in the cloud. In addition to integrating with ADFS, Preempt also integrates with Cloud SSO such as Okta and Azure SSO. This ensures you retain full context over all user activities whether the assets they use are on the on-premise network or in the cloud. Additionally staff can integrate policies between Preempt and Okta in order to ensure that on-premise controls follow a user to the cloud.

Security analysts can easily see all user behavior, challenge suspicious application behavior in the cloud, and identify risky configurations such as service accounts active in the cloud. Preempt also supports AWS and Azure Virtual Private Cloud (VPC) deployments. This allows Preempt to grow in lock step with your network whether on premise or in the cloud, and retain the same visibility, policy enforcement, and threat prevention.

Extending Beyond Access to Threat Prevention

For many organizations the move to the cloud has been focused on the basics of simply controlling access. And while access controls are obviously essential, Preempt allows organizations to do much more. First, access can be addressed in a dynamic and adaptive way. Instead of a one-time allow/deny decision, access decisions can adapt to the situation. As observed risks change, the solution can challenge a user in real-time to verify identity. Additionally, the solution can identify signs of malicious or attack behavior such as lateral movement, signs of compromised credentials, privilege escalation or dangerous tools and protocols. This ensures that instead of simply focusing on access, organizations can extend their full capability of threat prevention to the cloud as well.

About Preempt

Preempt protects enterprises from security breaches and malicious insiders with an innovative and patented approach based on Identity, Behavior, and Risk coupled with Adaptive Response to provide the most proactive solution for both detecting and automatically responding to security threats.

Learn more about us at www.Preempt.com