PREEMPT FOR OKTA

Optimize your Okta Deployment with Preempt's Threat Detection and Prevention Capabilities

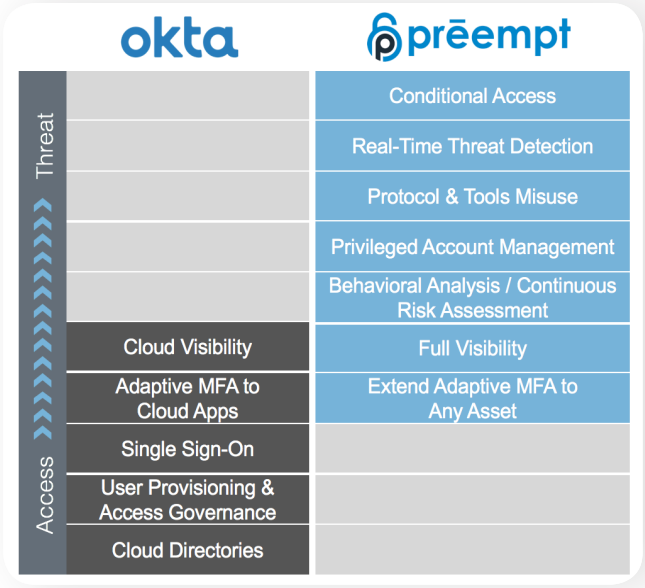
The Challenge:
Increasing Attack Surface & Disjointed Solutions

A growing threat landscape and more sophisticated cyberattacks means security teams need more proactive ways to protect the organization without disrupting business. At the same time, mobile users and the proliferation of cloud applications has undermined the network perimeter. To protect against all unauthorized access, security teams have been forced to implement disjointed point solutions, causing gaps in visibility and a lack of centralized control.

Organizations need a solution that can provide full visibility for threat detection and prevention - both on-premises and in the cloud - to address the increasing attack surface.

The Solution: Unified Visibility and Conditional Access

By integrating Preempt and Okta, security teams get visibility into all corporate applications, whether deployed on-premises or in the cloud. In addition, organizations can automatically respond to targeted attacks without disrupting day-to-day operations.



Preempt + Okta Single Sign On

- Unify visibility of all user behavior on-premises and in the cloud
- Track user application usage and challenge risky behavior
- Find risky usage of service accounts

Preempt + Okta Adaptive MFA

- Challenge accounts that may be compromised
- Automate detection and response
- Educate and empower end users

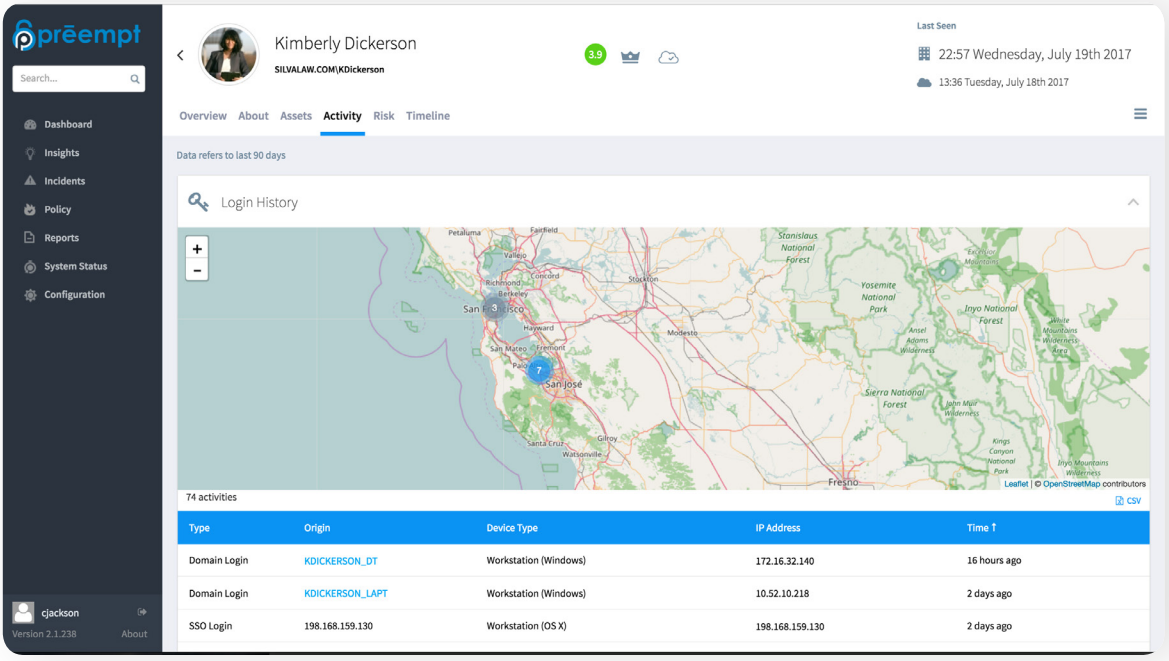
Enhancing Security Both On-Premises & In the Cloud

Unified Visibility & Conditional Access

Preempt continuously monitors and learns the behavior of all users, privileged users, service accounts and devices to identify risky activity and potential threats such as compromised credentials, malware or ransomware, lateral movement attacks, or malicious insiders. However, continuous detection is just the first step. By integrating with Okta's Adaptive Multi-Factor Authentication (Okta Verify with Push or Okta Verify with OTP), the Preempt Policy Engine can create an MFA challenge based on risk. Depending on the risk, the policy engine can either approve and auto-resolve the security incident or take a different action such as a step-up challenge or blocking the user.

Next, integration between Preempt and Okta's Single Sign-On (SSO) allows organizations to extend visibility and threat detection capabilities to their web and cloud-based applications. The Okta SSO connector allows Preempt to track and learn user behavior on any application that uses Okta's SSO. This provides security teams with a unified view of a user's behavior both on-premises or in the cloud.

For example, when analyzing a potentially compromised user account, security teams can quickly determine if the user has access to sensitive cloud applications to better contextualize risk to the organization. Security teams can see a unified view of all the user's application usage both in the cloud and on the local network, and set policies to enforce adaptive, risk-based authentication based on the user's context.



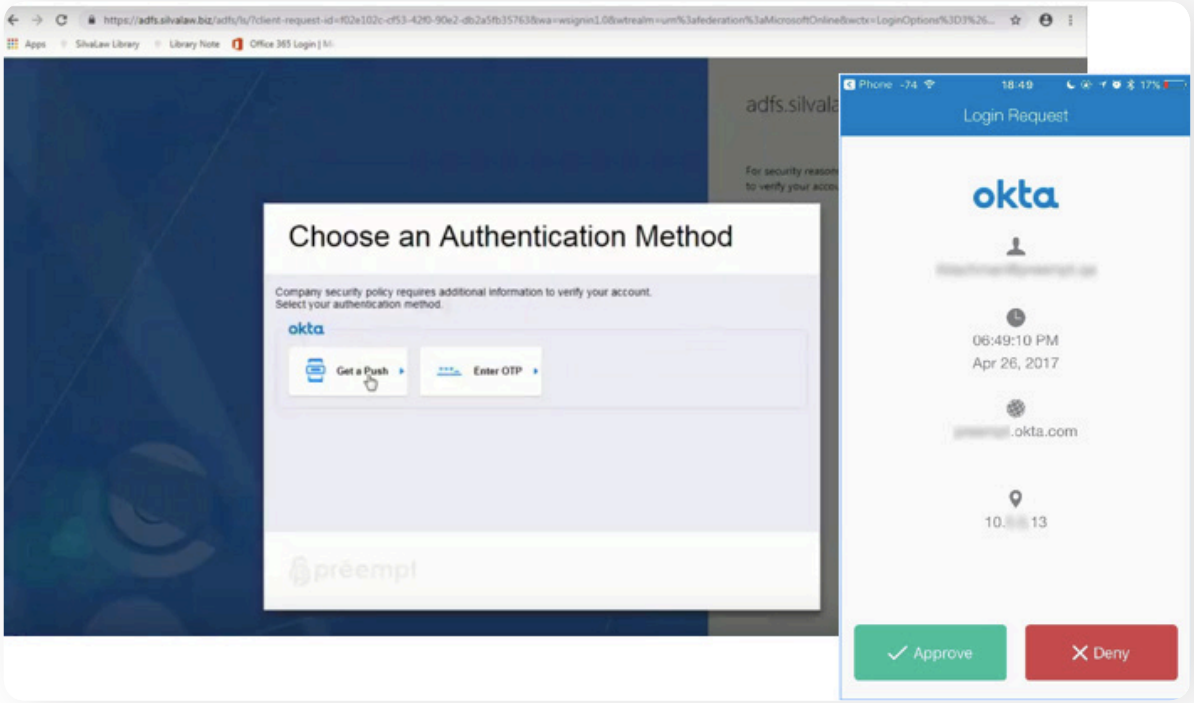
Get unique value with Preempt for Okta through these use cases

Enforcing Context-Aware MFA

Trigger MFA adaptively based on changing risk or threat context. Implementing adaptive MFA is critical for protecting against credential compromise, as user credentials are still the #1 target for attackers seeking access to sensitive systems and applications. Preempt automatically detects risky behavior, such as unknown endpoints accessing critical servers or threats like the presence of a stealthy administrator in a network. Once potentially malicious activity is detected, Preempt then triggers an Okta MFA challenge based on risk or policy.

Apply SSO Polices Based On Risk

Leverage Preempt's threat detection capabilities to update and fine-tune your Okta Single Sign On (SSO) policies for users and groups. Uniquely with the Preempt Platform, you can prevent threats such as lateral movement and unauthorized access. Preempt leverages proprietary pattern recognition and analytics to detect the misuse of hacking tools (eg. Mimikatz, Bloodhound, etc) in order to help organizations stop attacks such as Kerberoasting, Pass-the-Hash, and Golden Ticket. When risky behavior is spotted, you can create risky user groups to set and enforce appropriate policies that help respond to incidents and thereby get a faster resolution.



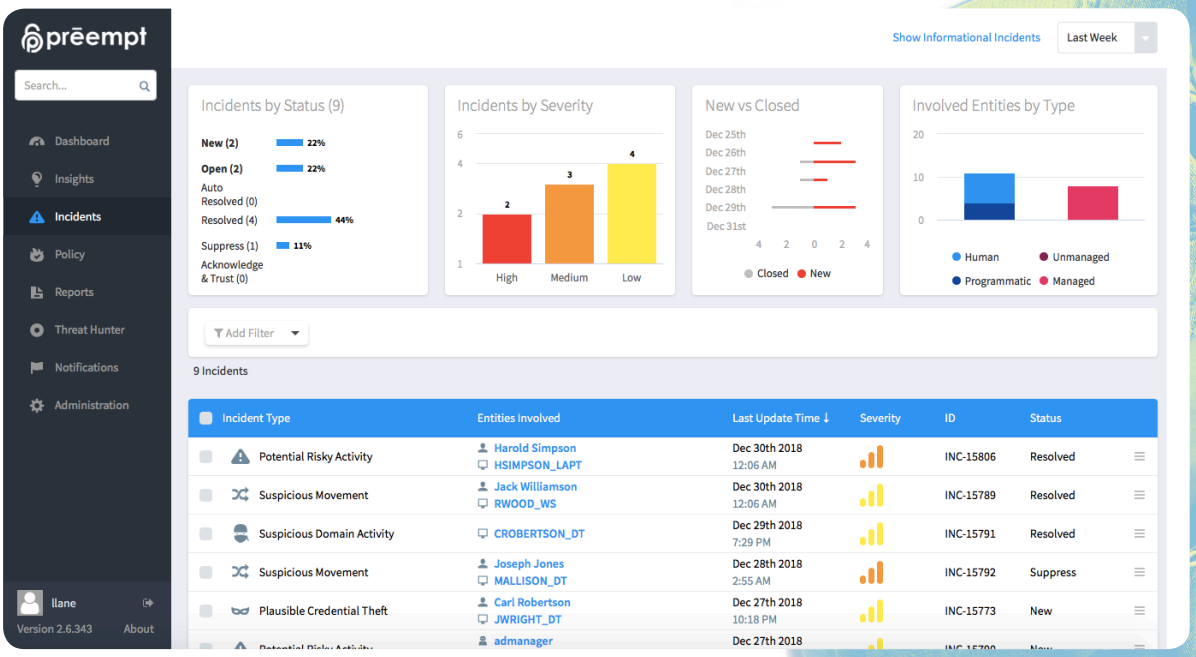
Extending Secure Access to All Network Assets

Preempt can enable multi-factor authentication in front of virtually any network asset including proprietary and custom systems, servers, devices, and applications that Okta does not support. Essentially any network-level authentication or authorization to the domain controllers (e.g. through a Powershell tool) can be protected with strong authentication through Preempt without the need for an invasive agent. For example, Okta customers who deployed Preempt can enforce secure local login to sensitive domain-joined workstations by requiring an out-of-band push notification before they are allowed access. By using Preempt, organizations can easily add adaptive authentication based on risk-scoring or policy (to their workstations, systems, and applications) without requiring any changes or customization to the applications themselves.

Enabling Unified Visibility Across the Environment

Get full visibility of user behavior, risks, and threats both on-premises and in the cloud. Preempt breaks downs silos by allowing you to get a complete understanding of your risky accounts in one central location so that you can take actionable steps to preempt threats.

With a single easy-to-use management console, Preempt provides a continuous health and risk assessment - revealing password problems, privileged access abuse, stealthy admins, Active Directory (AD) configuration issues, and more - so that you can gain more control over all accounts and use that visibility to provide true threat intelligence and risk insight.



preempt

www.preempt.com info@preempt.com

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.