okta

Identity Threat Protection with Okta AI

Unify risk insights and continuously assess and respond to identity threats in real-time, during and after login

Identity is a top attack vector. As organizations step up their Identity security, threat actors are responding with new ways to breach defenses, including credential theft, privilege abuse, and session hijacking. Focusing on a single threat surface is not enough - just as attackers target multiple surfaces, defenders must also take a holistic approach to identity security, leveraging signals from vendors that protect these diverse attack surfaces to eliminate silos and administrative gaps. Effective response requires early action at the identity layer, controlling access, and Okta, as an identity provider, delivers real-time inline protection to swiftly detect and mitigate identity threats.

okta

Overcoming Fragmented Security Views and Balancing Security with Usability

Security teams often struggle with fragmented visibility across disparate security solutions, making it challenging to effectively detect and respond to identity threats. Siloed tools and lack of integration lead to blind spots, increased workload, and slower threat response times. Additionally, organizations must strike a balance between enforcing strong security measures and maintaining a seamless user experience. Overly strict policies can hinder productivity and cause user frustration, while overly lax policies leave the organization vulnerable to attacks.

Okta Identity Threat Protection (ITP) with AI addresses these challenges by providing holistic visibility into identity risk, leveraging Okta's unique position as your IdP. With visibility into the authentication patterns across diverse environments, Okta has an informed understanding of what it believes is normal and anomalous behavior. By applying advanced AI and machine learning to this rich identity data, Okta can detect even subtle changes in risk, such as variations in IP addresses, to identify potential threats in real-time. It's important to note that what Okta identifies as anomalous behavior may turn out to be normal, and vice versa.

Further, integrating insights from your existing security tools, allows for a comprehensive view of risk, enabling streamlined investigations and automated responses. Okta's scale and focus on being "always on, always secure" for the world's largest organizations powers this uniquely effective approach to identity threat detection and response.

Why Use Identity Threat Protection?

Part of Okta's Workforce Identity Cloud, ITP is a suite of capabilities in the Workforce Identity Cloud that strengthens your identity security posture and enables continuous, real-time threat detection and response throughout the user journey. Unlike other Identity Threat Detection and Response (ITDR) solutions that rely solely on integrations with the IdP, Identity Threat Protection is built natively into Okta, which allows ITP to operate at the critical access control point while still leveraging integrations with security providers to enhance threat visibility. By doing so, ITP expands your view across your identity threat surface without relying exclusively on these IdP integrations, providing more comprehensive threat detection and response. This unique position empowers Okta to detect identity threats in real-time and allows you to rapidly remediate compromised identities. By enabling you to configure actions, such as blocking users when a threat is detected, ITP significantly enhances your security posture with unmatched efficiency and effectiveness.

Key Business Outcomes

Stronger security posture
Use insights from Okta and your existing security tools to continually assess users and their sessions for risk and proactively harden your identity security posture

Faster threat detection and response
Leverage Identity threat analytics, Okta AI, and third-party signals to detect Identity-related threats like session hijacking in real-time and configure Identity Threat Protection to respond automatically when it detects a threat.

Maximize value of security investments
Send and receive relevant security events from tools you already have to gain a holistic view of user risk and get more value out of your existing security stack

Better user experience
Enable long-lived sessions but use Identity Threat Protection to help detect and automate your responses to threats in real-time to minimize therisks associated with long-lived sessions and tailor actions based on changes in user or session threat levels to balance security and convenience

okta

Okta's Risk Engine can detect threats like:


Session hijacking


MFA brute force


Application session cookie harvesting


Access attempts from phishing infrastructure


User-reported anomalous behavior


Attempts to achieve privilege escalation from high-risk IPs


Lateral movement informed by 3rd party signals

How It Works

Identity Threat Protection leverages Okta risk signals alongside integrations with top security providers to provide real-time detection, continuous assessment, and automated responses, as configured by you, to identity threats, unifying risk insights and enhancing security at the identity layer.

Continuous Risk Evaluation

While risk-based authentication and common ITDR approaches can consider post-login factors, they often lack the depth, granularity, and inline action capabilities of a native, universally integrated cloud IdP like Okta. Identity Threat Protection continuously evaluates the risk of all users and their sessions against policies configured by your admins, using information such as:

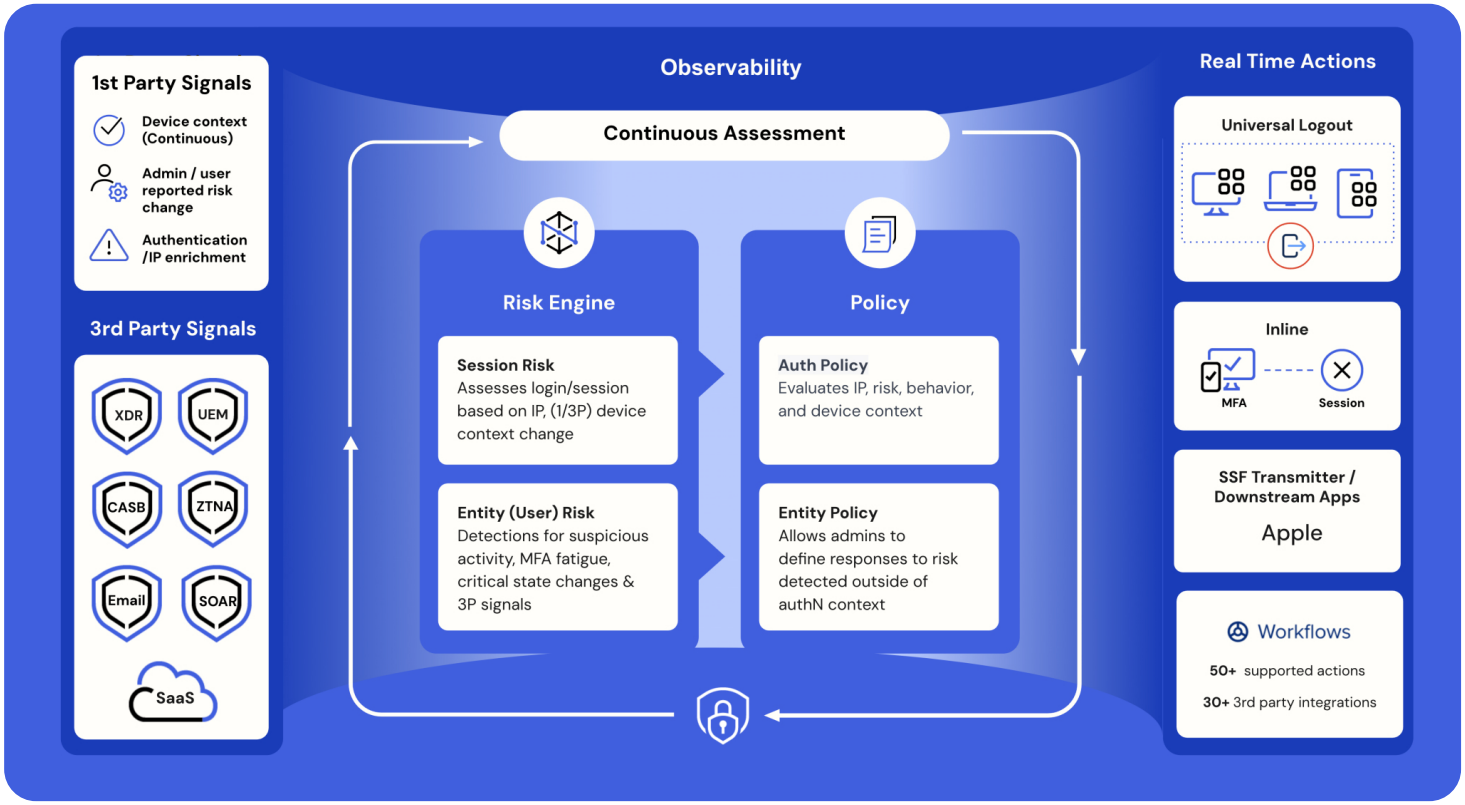
- **Session Risk Detection**
  Advanced machine learning models continuously evaluate every authentication request post-authentication to detect identity risks, such as session hijacking attempts, leveraging Okta's vast visibility into authentication patterns.
- **Entity Risk detections**
  Protection against identity-based attacks like brute force and credential harvesting
- **Context-Aware Device and IP Protection**
  Risk analysis using device context continuously monitored by Okta, including re-evaluating existing Okta Verify configurations and leveraging Device Assurance policies to ensure comprehensive security.

Shared Signals Pipeline

Beyond continuously evaluating risk with its own data, Okta also integrates insights from other best-in-class security technologies to expand your visibility into potential risks. Identity Threat Protection uses the OpenID Shared Signals Framework (SSF) to transmit and receive security event information from SaaS apps and third-party security technologies such as:

- **MDM**
- **CASB**
- **EDR/XDR**
- **UEM**
- **SASE**

Identity Threat Protection has out-of-the-box integrations with a wide range of best-of-breed security tools to provide the most comprehensive view of identity risk. Information such as elevated user privileges in an app, malware on a device, or a phishing email in a user's inbox could all signal the start of an Identity-related attack. With Identity Threat Protection continuously analyzing signals from across your security ecosystem, you gain unparalleled real-time visibility.



Continuous Risk Re-Evaluation

- **Dynamic Global Session & Auth Policy Re-evaluation**
  Persistently re-evaluates policies throughout the user's session to maintain security posture
- **Risk-Based Entity Access Policies**
  Enables granular, adaptive policies driven by real-time user and entity risk insights

Precision Risk Response

As your identity provider controls the authentication flow, Identity Threat Protection enables real-time, inline responses to detected threats. Identity threat response should be immediate, automatic, and tailored to the level of risk, so you can stop threats with minimal disruption to users and their work.

Adaptive actions in Identity Threat Protection enable you to tailor automated responses to changes in an entity's session or user risk level or the risk level of a particular session. Available adaptive actions include:

- **Universal Logout**
  Immediately clears sessions of supported apps and revokes tokens for a particular user upon detecting credential theft or session hijacking attempts
- **Inline MFA**
  Prompts a user to re-authenticate and/or steps up authentication for new sessions when risk levels increase
- **Security Workflows & Orchestration**
  Initiates workflows to respond to risk events, such as kicking off an investigation or limiting user access to view only in particular apps to contain potential threats.

As an SSF transmitter, Identity Threat Protection can also drive downstream actions in receiver systems. Just as partner solutions send signals and alerts to Okta, ITP can transmit risk insights to trigger responses in downstream applications and services. For example, ITP can instruct a workforce app to log out a high-risk user or signal to Apple Business Manager to restrict a compromised account.

Observability & Insights

Leveraging Identity Threat Analytics, ITP delivers visibility into threats and analyzes anomalies to enable rapid, effective response. It strengthens threat mitigation capabilities through actionable insights, giving security teams the tools they need to analyze and act upon threat data in a timely manner.

- **Risk Investigation Reports**
  Enable security analysts to efficiently triage and investigate identity-based threats
- **Security risk dashboards**
  Provide high-level overviews of identity risk posture and key metrics
- **Rich system logs**
  Capture detailed event data and the reasoning behind risk assessments for auditing and forensics

Getting Started

Identity Threat Protection is available with Okta Identity Engine and only available for Workforce Identity Cloud.