okta

Identity Threat Protection with Okta AI

Continuously assess and respond to identity threats in real-time

The rise of hybrid work has reinforced identity's pivotal role in modern security, making it a primary target for cyber threats. As organizations step up their identity security strategies, threat actors respond with new ways to breach defenses, including credential theft and session hijacking. Focusing on a single entry point is not enough - just as attackers target multiple surfaces, organizations must also take a holistic approach to identity security. Effective detection and response starts at the identity layer and demands real-time, inline actions to swiftly mitigate identity-based threats.

Smarter identity threat protection that doesn't slow your users down

As identity-based threats rise, fragmented visibility across disparate security tools leads to blind spots, increased overhead, and slower response times. Security teams must also balance strong protection with a smooth user experience. Too strict, and users are frustrated. Too lax, and the organization is vulnerable to attacks.

Identity Threat Protection with Okta AI (ITP) addresses these challenges with unified, context-rich visibility into user behavior and risk – during and after authentication. As the identity provider, Okta analyzes access patterns across diverse environments, establishing a baseline of normal user behavior to detect anomalies in real-time. Powered by Okta AI, ITP identifies subtle changes in user risk and behavior, such as unusual IP activity, and triggers adaptive actions to neutralize threats. By integrating with your existing security stack, it delivers a comprehensive view of user risk, accelerating investigations and automated response.

okta

Why use Identity Threat Protection with Okta AI?

ITP delivers continuous, real-time threat detection and response throughout the user journey. Unlike other solutions that focus primarily on securing the endpoint, ITP operates directly at the identity layer.

It uses native identity signals and integrates with the existing security tools you depend on to expand visibility across the threat surface. Automated actions – like blocking users, requiring step-up authentication, or logging users out of all their connected apps – enable rapid threat response and real-time remediation of compromised identities, strengthening your security posture with unmatched speed and precision.

Okta's Risk Engine can detect threats like

- Session hijacking
- MFA brute force
- Application session cookie harvesting
- Phishing attempts
- User and admin reported risk
- Attempts at privilege escalation from high-risk IPs
- Lateral movement across identity systems

Key Business Outcomes

Strengthen security posture

Continuously assess user context and risk during and after login to proactively harden your identity defenses and stay ahead of evolving threats.

Accelerate threat detection and response

Leverage identity threat analytics, Okta AI, and third-party signals to detect threats – like session hijacking– in real-time and configure automated responses to reduce manual effort and neutralize threats faster.

Maximize the value of security investments

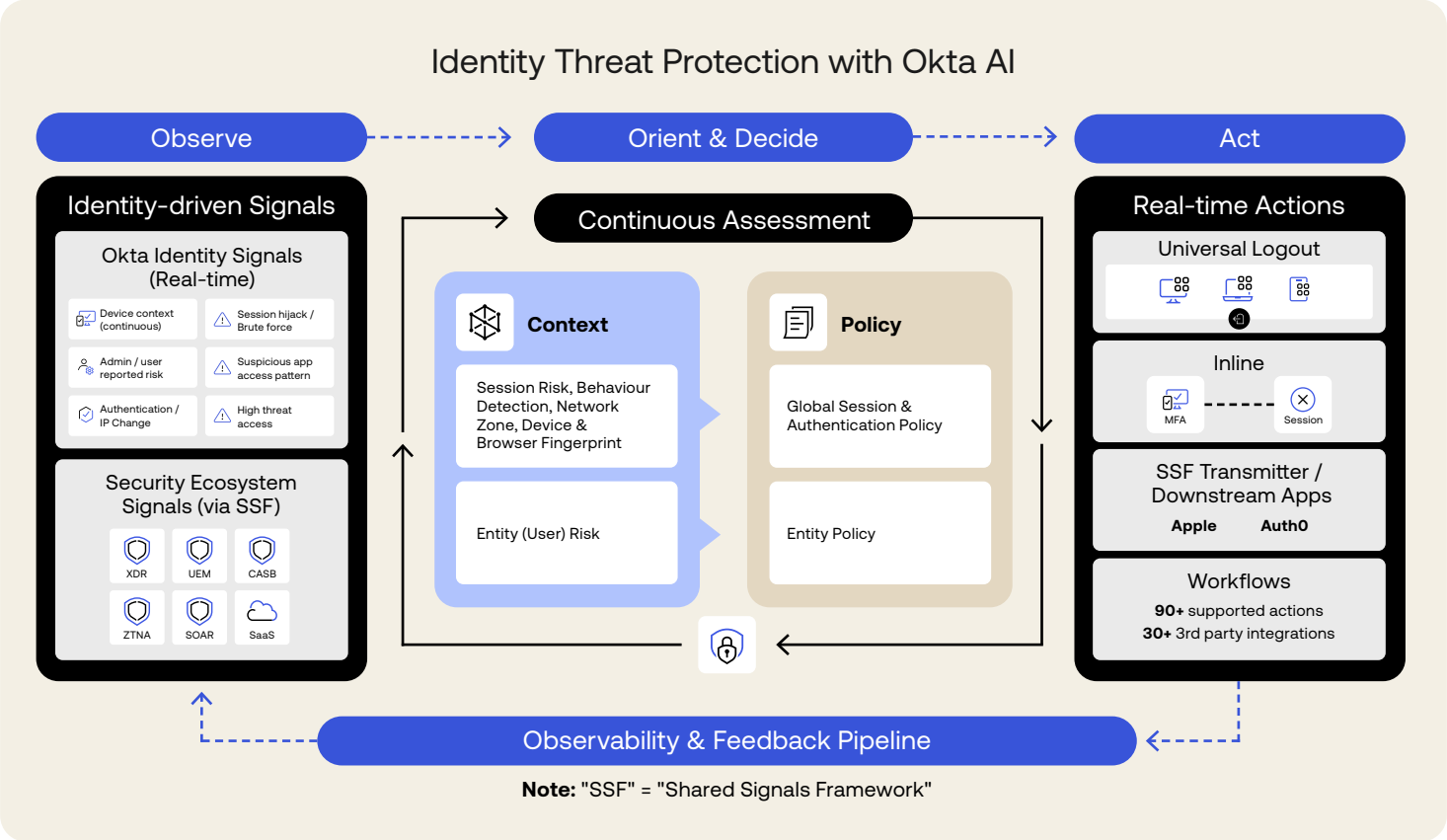
Seamlessly integrate with your current security ecosystem to gain a unified view of user risk and amplify the effectiveness of your existing security investments.

Deliver seamless yet secure user experiences

Reduce the friction of short-lived sessions and monitor for changes in risk with automated, tailored responses, balancing security and user convenience.

How it works

Okta analyzes risk and user context to deliver continuous, real-time threat protection. By unifying risk detections across your tech stack, Okta helps you defend against identity-based threats, such as MFA brute-force, session hijacking, and phishing attempts.



Continuous Context Evaluation

Okta helps maintain strong security throughout the entire user session by continuously assessing user risk using contextual signals and advanced detection models, such as:

Session risk

Sophisticated risk models monitor for signs of compromise, by analyzing authentication behavior, context changes, and anomalies in real-time, even after successful login.

Entity risk

Continuously evaluates each user's overall risk profile based on historical behavior, recent activity, and potential indicators of compromise—enabling policies to dynamically adjust as risk changes.

Device and IP risk

Tracks device posture and IP reputation throughout the session, using Okta Verify configurations and Device Assurance policies to identify anomalous behavior that could signal elevated risk.

okta

Shared Signals Ecosystem

In addition to our native identity signals, Okta leverages the OpenID Shared Signals Framework (SSF) to exchange security event data with SaaS applications and leading security tools, such as:

MDM | UEM | EDR/XDR | SASE/SSE | ZTNA | SOAR | CASB | SSPM | BDR

Information such as elevated user privileges in an app, malware on a device, or a phishing email can signal the start of an identity-related attack. With Okta continuously analyzing signals across your security ecosystem, you gain a comprehensive view of identity risk and can stay ahead of threats before they escalate.

Dynamic Policy Evaluation

When Okta detects changes in behavior, device posture, or threat level, it evaluates those changes against your policies, and takes real-time action, stopping threats as they surface and before they infiltrate your systems. This includes:

Global session & authentication policy evaluation

Continuously re-evaluate policies throughout the user session to maintain security posture

Entity risk policy

Enforce adaptive, context-aware policies that adjust access decisions based on user risk, as threats evolve

Precision Risk Response

Building on dynamic policy evaluation, Okta enforces granular, inline responses the moment risk levels change – targeted to the specific user, session, or scenario. These real-time actions help neutralize threats quickly, while minimizing disruption for legitimate users. Adaptive actions include:

Universal Logout

Instantly clears active sessions and revokes tokens across all supported devices and applications when high-risk behavior for a particular user is detected.

Inline MFA

Prompts for re-authentication and/or step-up MFA based on session, user, and environmental context, ensuring access remains appropriate to the current threat level.

Security workflows & orchestration

Triggers automated, multi-step responses to risk events, such as restricting app permissions, initiating investigations, or notifying security teams.

As an SSF transmitter, Okta can drive additional actions to downstream applications and services. Beyond the identity layer, Okta's role as a transmitter extends rich security intelligence to connected systems like Apple Business Manager, facilitating more robust and context-aware security responses.

Identity Threat Analytics

Okta gives security teams the visibility they need to detect, investigate, and respond to identity threats more effectively. With clear insights and detailed context, teams can act quickly and confidently.

Risk investigation reports

Enables analysts to efficiently triage and investigate identity-based threats with detailed insights into user behavior and activity.

Security risk dashboards

Provides a holistic view of identity risk across your environment, making it easier to spot trends, track key metrics, and adjust security policies as needed.

Rich system logs

Captures detailed event data and the reasoning behind risk decisions to support compliance audits and forensic analysis.

Feedback Pipeline

Admins can also provide direct feedback to help fine-tune detections, improving the accuracy of risk assessments over time. Through model feedback and labeling, customers play an active role in refining Okta's detection models. This collaboration between human expertise and AI helps reduce false positives and ensures the system stays aligned with the organization's operational baseline and overall security posture.

> "The seamless integration of ITP into our existing systems, coupled with Okta's great support, accelerated our time to value and strengthened our security posture. We used to spend hours each day investigating threats. With Okta, we've put time back in our days to focus on more strategic IT initiatives that drive more business value."

Will Freeman
IT Systems Engineer, Sign In Solutions

Sign In Solutions

Getting Started

Identity Threat Protection is available with Okta Identity Engine for Okta Workforce Identity customers. Ready to stop identity threats before they occur? Talk to an expert today.

About Okta
Okta is the World's Identity Company. As the leading independent Identity partner, we free everyone to safely use any technology—anywhere, on any device or app. The most trusted brands trust Okta to enable secure access, authentication, and automation. With flexibility and neutrality at the core of our Okta Workforce Identity and Customer Identity Clouds, business leaders and developers can focus on innovation and accelerate digital transformation, thanks to customizable solutions and more than 7,000 pre-built integrations. We're building a world where Identity belongs to you. Learn more at okta.com.