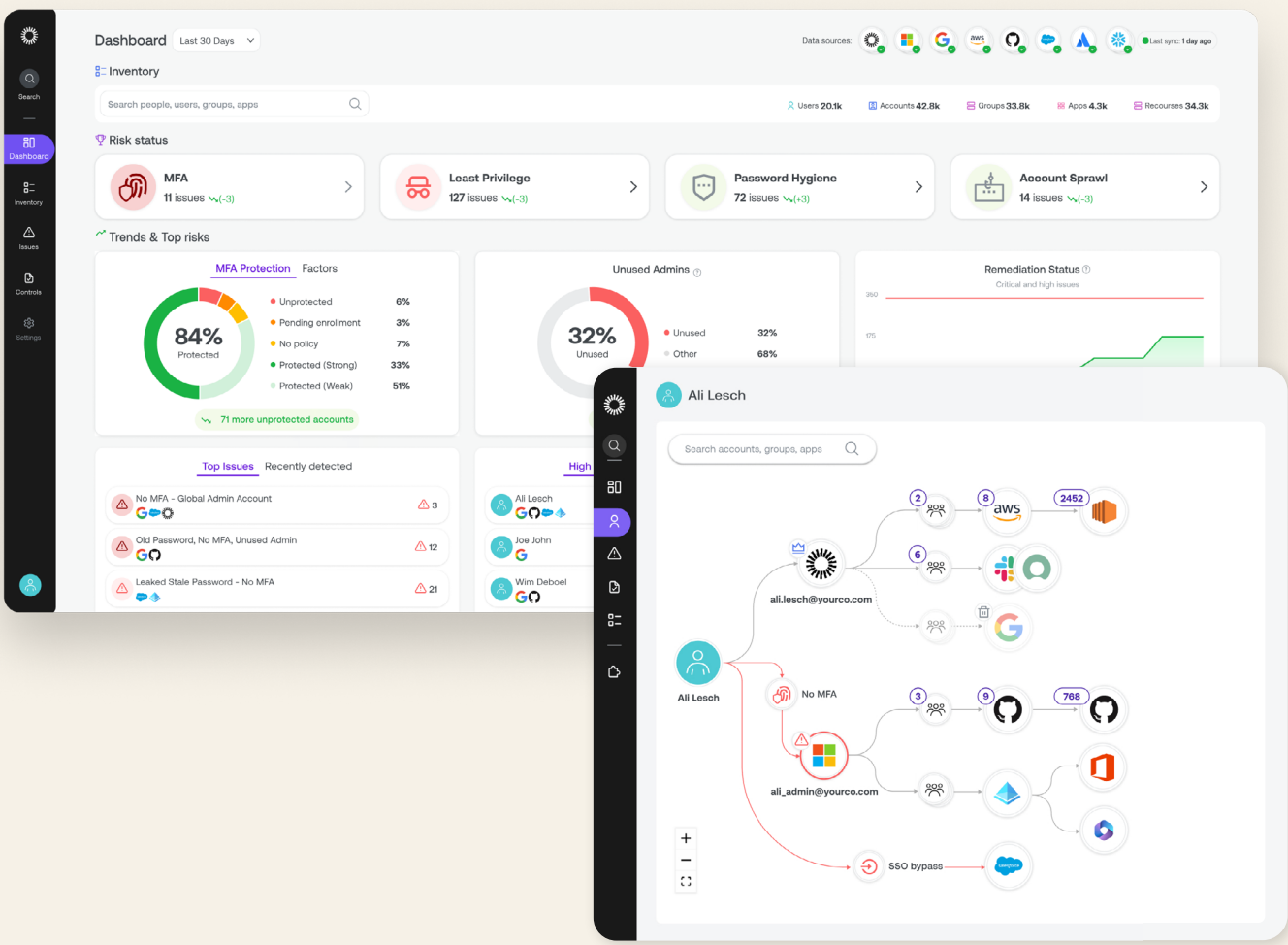
Okta Identity Security Posture Management

See, understand, prioritize, and remediate identity threats using Okta's robust Identity Security Posture Management (ISPM) solution.

The identity and access sprawl has become an expansive, unmanaged attack surface rife with partially offboarded users, over-provisioned identities, and unused and risky permissions.

This precarious reality exposes organizations to malicious access via phishing as well as stolen credentials and account takeovers, draining the time and resources of security teams charged with protecting them.



> "This year (2022) 82% of breaches involved the human element. Whether it is the Use of stolen credentials, Phishing, Misuse, or simply an Error, people continue to play a very large role in incidents and breaches alike."
>
> Verizon 2022 Data Breach Investigation Report

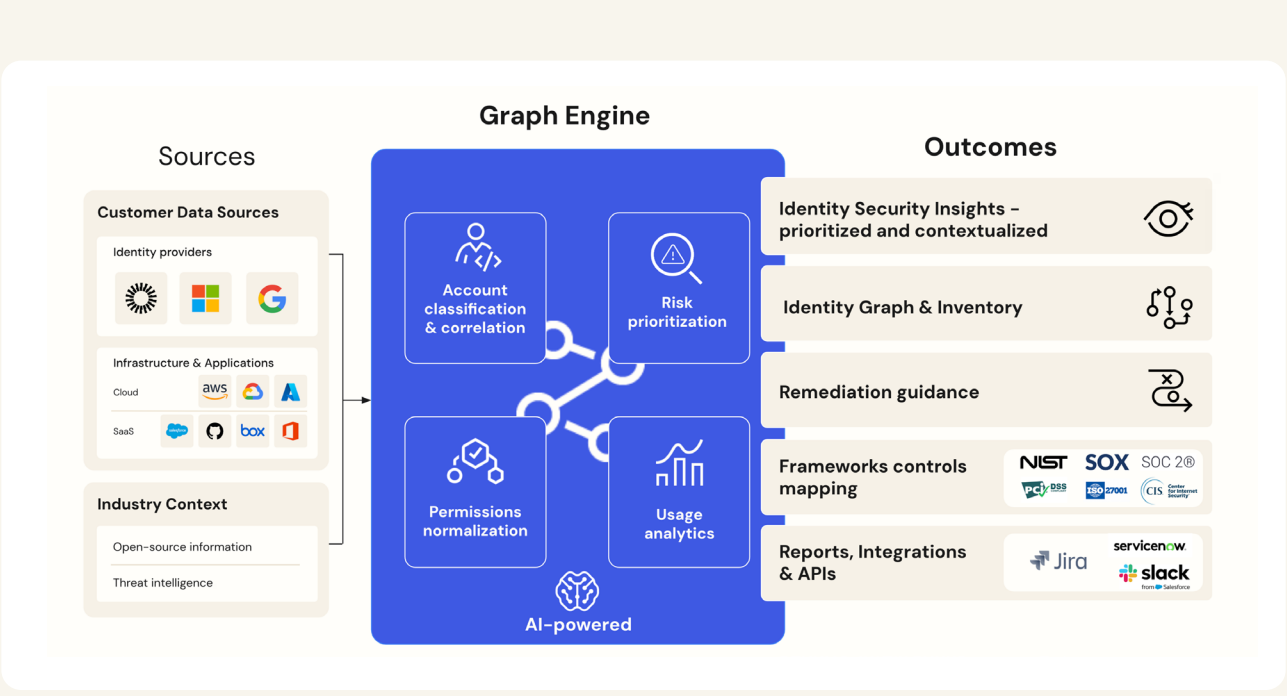
Counter Identity-based Threats

Our solution is a single and streamlined offering that automates identity visibility, management and remediation. This delivers a "one- stop-shop" for identifying identity risk and prioritizing it. In addition, the product's unparalleled contextualization capabilities link all user accounts to their required privileges, activities, and stage in the employee lifecycle to mitigate threats and support compliance.

Okta's customers report that 75% of critical identity issues were resolved within several weeks following a quick deployment.

Okta ISPM Architecture

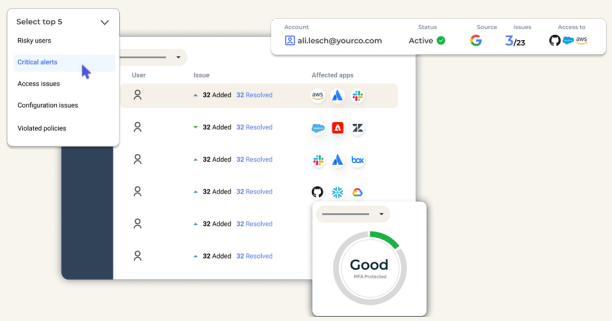
Okta ISPM identity graph engine connects to a variety of identity data, breaking the silos and building context rich visibility. As a result, security teams are empowered to make the right decisions that will improve their overall identity security posture.



How Okta ISPM Works

Fast and Easy Integration

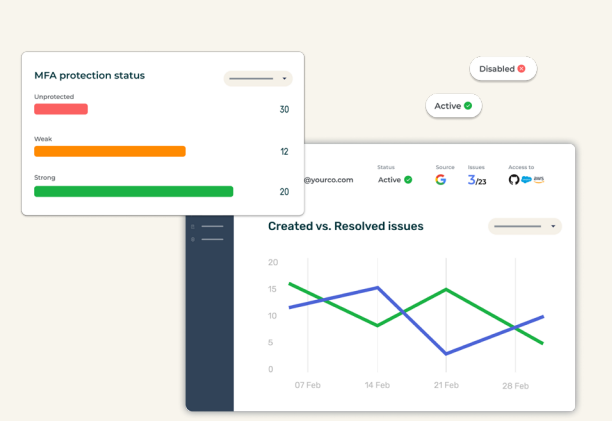
An easy, agentless process seamlessly integrates with your identity providers and both cloud and on-prem applications and creates a snapshot of the identity attack surface.



Classification & Prioritization

Our Identity Schema normalizes data and performs risk classification in the usage analysis.

Next, the Identity and Access Graph contextualizes the data and prioritizes identity issues based on severity and risk, leading to effective remediation.



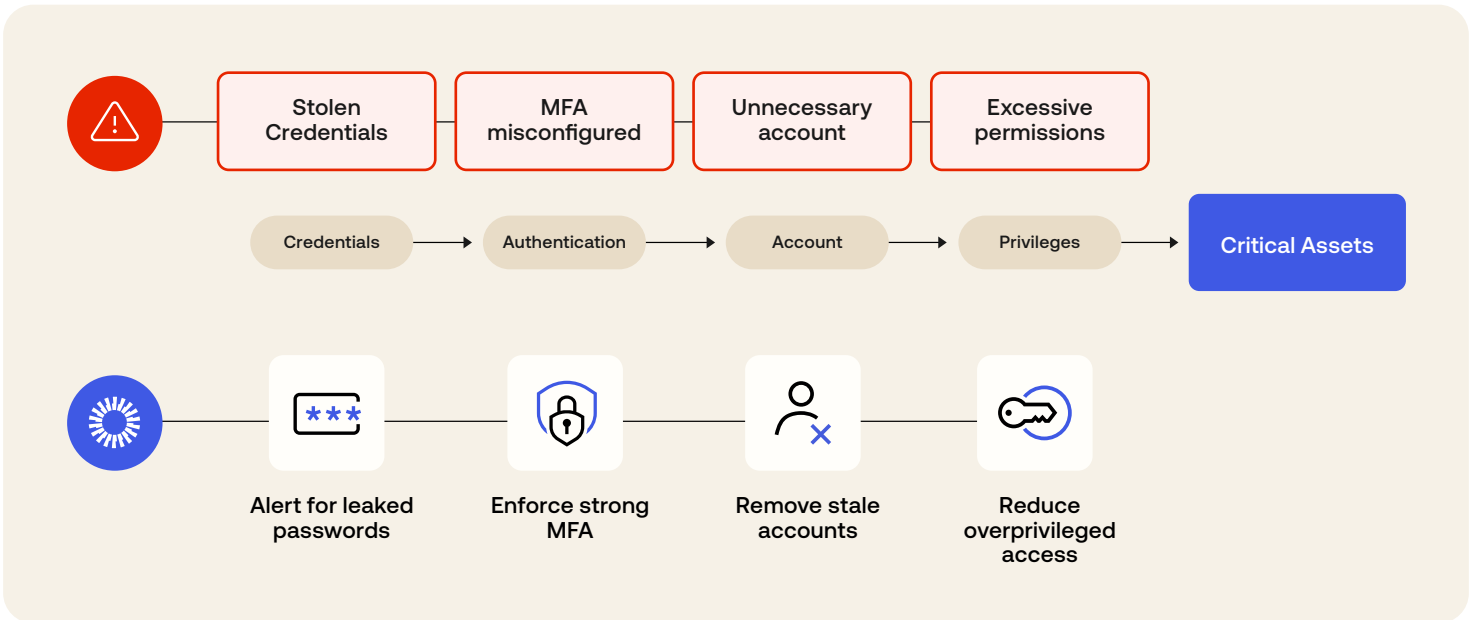
Remediation, Monitoring & Reporting

By applying critical context and actionable insights to its remediation processes, Okta ISPM strengthens identity postures without jeopardizing business.

The ongoing process detects issues and recommends resolutions that prevents new threats, ensures that identity policies are implemented, and tracks least-privilege metrics.

A Complete Identity Journey

The solution covers and automates critical aspects of identity security management, from alerts to analysis and remediation to protection. Security teams can fix problems before they become breaches, identify and correct identity processes and product implementations to minimize future issues, and provide continuous posture, compliance, and audit data to the business.



How Okta ISPM Can Help?

Okta ISPM helps protect enterprise-critical assets and customer data across key aspects of the attack surface

Control admin sprawl

Automatically identify privileged accounts and alert security teams of their existence, then drive prioritization and remediation.

Validate and strengthen MFA coverage

Analyze the company's Identity Graph and continuously highlight any new apps and resources that can be accessed without MFA.

Validate offboarding

Easily determine which privileges have been given to offboarded users and reduce the time needed to complete the offboarding process while continuously supporting compliance.

Okta ISPM facilitates identity collaboration across the enterprise

Identity security teams

Okta ISPM dramatically reduces risk from access sprawls, eliminates manual tasks, and significantly reduces the risk inherent in human error with comprehensive coverage. Security teams are empowered with consolidated, end-to- end visualizations with rich context across systems and people - crucial for identifying risk and prioritizing it.

CISOs

CISOs can mature their identity security program and measure, monitor, and improve their security posture. Resolving one of the industry's most pressing (and growing) attack vectors, our ISPM solution minimizes inter- organizational dependencies and facilitates continuous policy adherence, compliance, and board requirements.

IT teams

IT teams gain control and a complete map of business requirements in accordance with actual access provisioning. As a result, IT teams improve the efficiency of identity operations as well as the end-user experience.

Business leaders

Business executives will benefit from the ability to reduce the risk of breaches while helping validate compliance with identity regulations. ISPM minimizes friction and resolves any misalignments between IT and security teams while saving costs and resources spent on licenses.

Application administrators

Application admins have access to easy-to-understand guidelines and best practices to improve and strengthen their identity security and can help preventing the next breach from targeting their apps. Using integrated reporting capabilities, admins are empowered to implement effective identity compliance on an ongoing basis, and eliminate tedious tasks relevant to user access reviews.

About Okta

Okta is the World's Identity Company. As the leading independent Identity partner, we free everyone to safely use any technology. 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.