Generative AI in Identity and security: the potential and the risks

Philip Hoyer
Field CTO, EMEA, Okta

Safe harbor

This presentation contains “forward-looking statements” within the meaning of the “safe harbor” provisions of the Private Securities Litigation Reform Act of 1995, including but not limited to, statements regarding our financial outlook, long-term financial targets, product development, business strategy and plans, market trends and market size, opportunities, positioning and expected benefits that will be derived from the acquisition of Auth0, Inc. These forward-looking statements are based on current expectations, estimates, forecasts and projections. Words such as “expect,” “anticipate,” “should,” “believe,” “hope,” “target,” “project,” “goals,” “estimate,” “potential,” “predict,” “may,” “will,” “might,” “could,” “intend,” “shall” and variations of these terms and similar expressions are intended to identify these forward-looking statements, although not all forward-looking statements contain these identifying words. Forward-looking statements are subject to a number of risks and uncertainties, many of which involve factors or circumstances that are beyond our control. For example, the market for our products may develop more slowly than expected or than it has in the past; there may be significant fluctuations in our results of operations and cash flows related to our revenue recognition or otherwise; we may fail to successfully integrate any new business, including Auth0, Inc.; we may fail to realize anticipated benefits of any combined operations with Auth0, Inc.; we may experience unanticipated costs of integrating Auth0, Inc.; the potential impact of the acquisition on relationships with third parties, including employees, customers, partners and competitors; we may be unable to retain key personnel; global economic conditions could worsen; a network or data security incident that allows unauthorized access to our network or data or our customers’ data could damage our reputation and cause us to incur significant costs; we could experience interruptions or performance problems associated with our technology, including a service outage; the impact of COVID-19 and variants of concern, related public health measures and any associated economic downturn on our business and results of operations may be more than we expect; and we may not be able to pay off our convertible senior notes when due. Further information on potential factors that could affect our financial results is included in our most recent Quarterly Report on Form 10-Q and our other filings with the Securities and Exchange Commission. The forward-looking statements included in this presentation represent our views only as of the date of this presentation and we assume no obligation and do not intend to update these forward-looking statements.

Any unreleased products, features or functionality referenced in this presentation are not currently available and may not be delivered on time or at all. Product roadmaps do not represent a commitment, obligation or promise to deliver any product, feature or functionality, and you should not rely on them to make your purchase decisions.

Mainframe

Personal computing

Client-server

Internet

Every company is an technology AI company

Every company is a technology company

Every company is an technology AI company

What's your
AI strategy?

What markets are
you playing in?

What advantages
does this give you?

> By 2025 at least 35% of organisations will utilise generative AI as part of their identity fabric functions. These organisations will substantially improve user experience and efficiency of their IAM controls.
>
> **Gartner**

Source: Gartner “Identity and Access Intelligence Innovation With Generative AI” by Homan Farahmand

okta

Organisations

Proactive security

Customers

Frictionless user experience

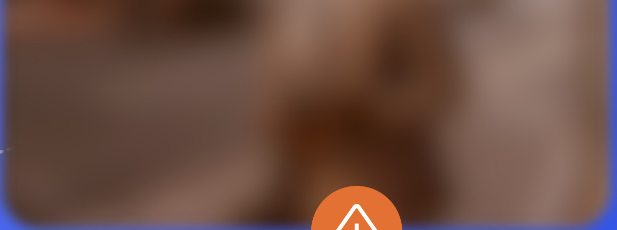
Developers

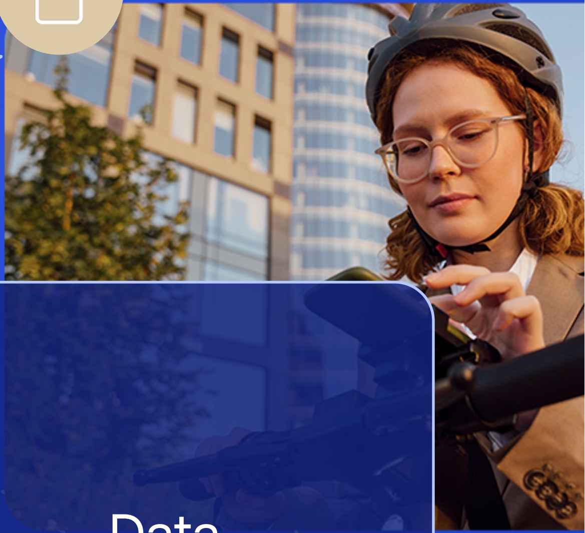
Build apps faster

Extended workforce

Efficient workflow automation

Generative AI is not only a solution… but also is driving new security risks



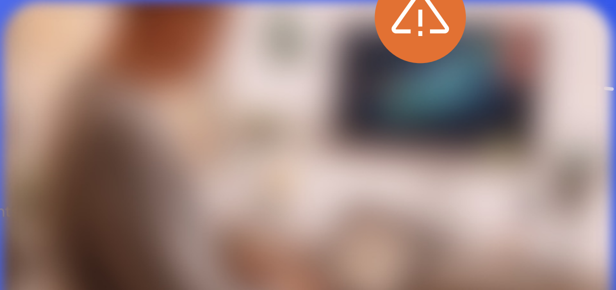


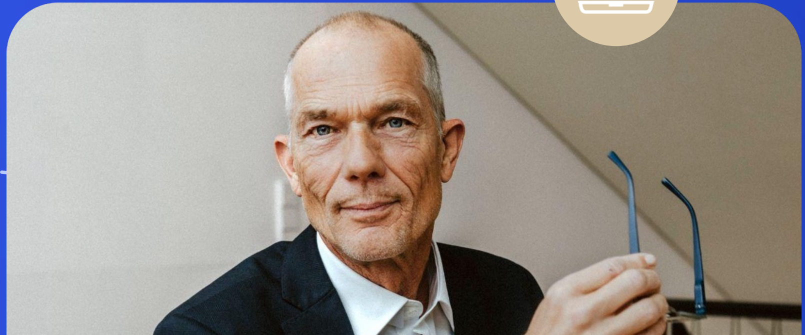
Attacking with more ‘swords’

Automating Request Floods (DDoS)

API and service risks

Data volume





Most common attacks in 2023...

Tech support scams: pretending to be Apple, Microsoft, Norton... etc.

Coworker impersonation: IT, Executives, member of your team

Bank impersonation: pretending to be loss prevention

47%

increase in phishing

Zscaler 2022 Threat Labz Phishing Report

Drive IT Leaders to change priorities!

The stakes are high

$1.87b

Session cookies harvested, tied to Fortune 1000[1]

63%

Breaches reported by external agencies[2]

$1.76m

Savings for those who use tooling that employs AI/ML[3]

[1] Spycloud (2023) Fortune 1000 Identity Exposure Report, [2] Mandiant (2022) Mandiant M-Trends 2022: Insights into Top Cyber Trends and Attacks, [3] IBM (2023) Cost of a Data Breach Report.

Lots of AI buzzwords, but what does it all mean?

ChatGPT

Machine learning

Predictive analysis

Optimisation

Data science

Computer vision

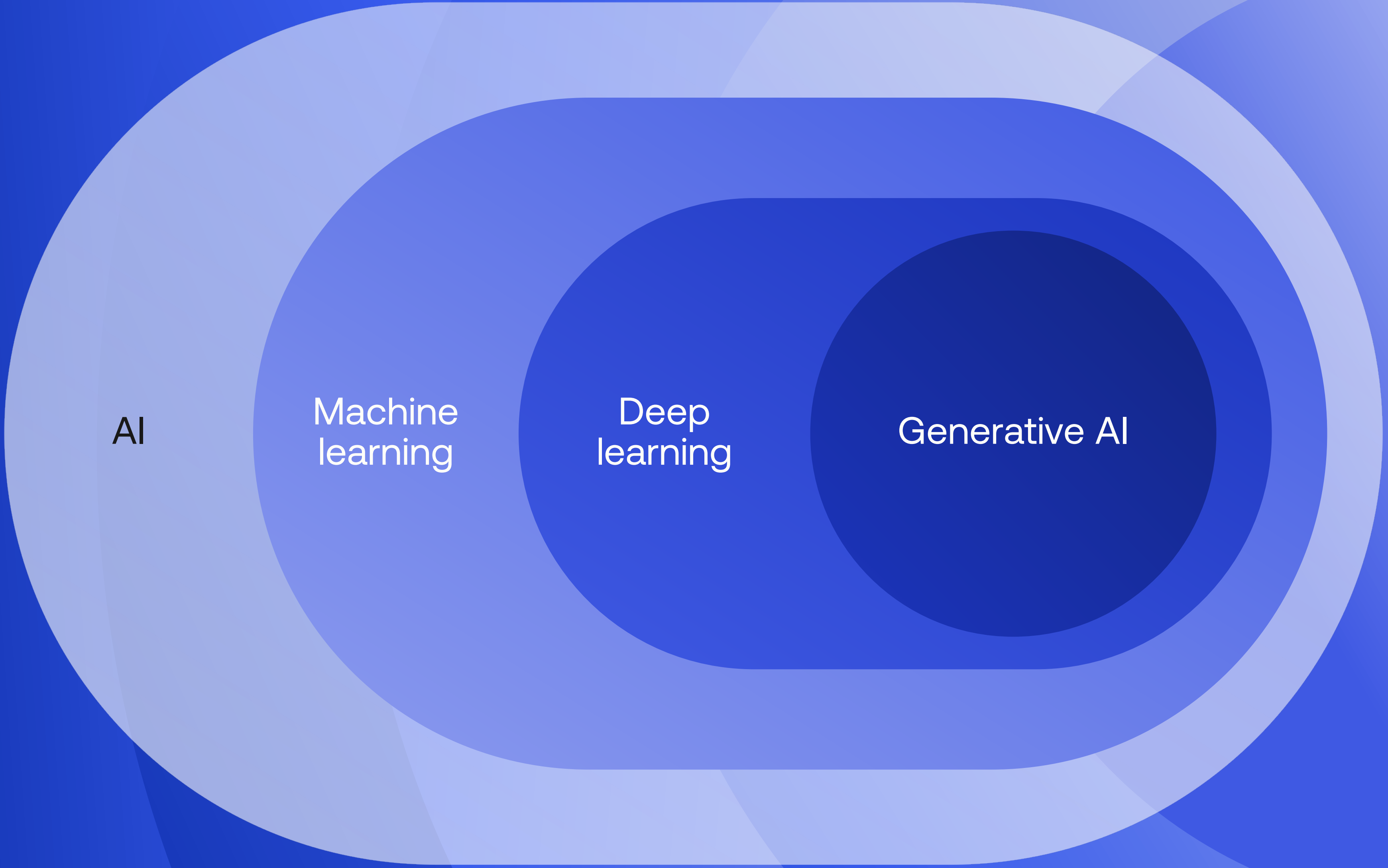
Data mining

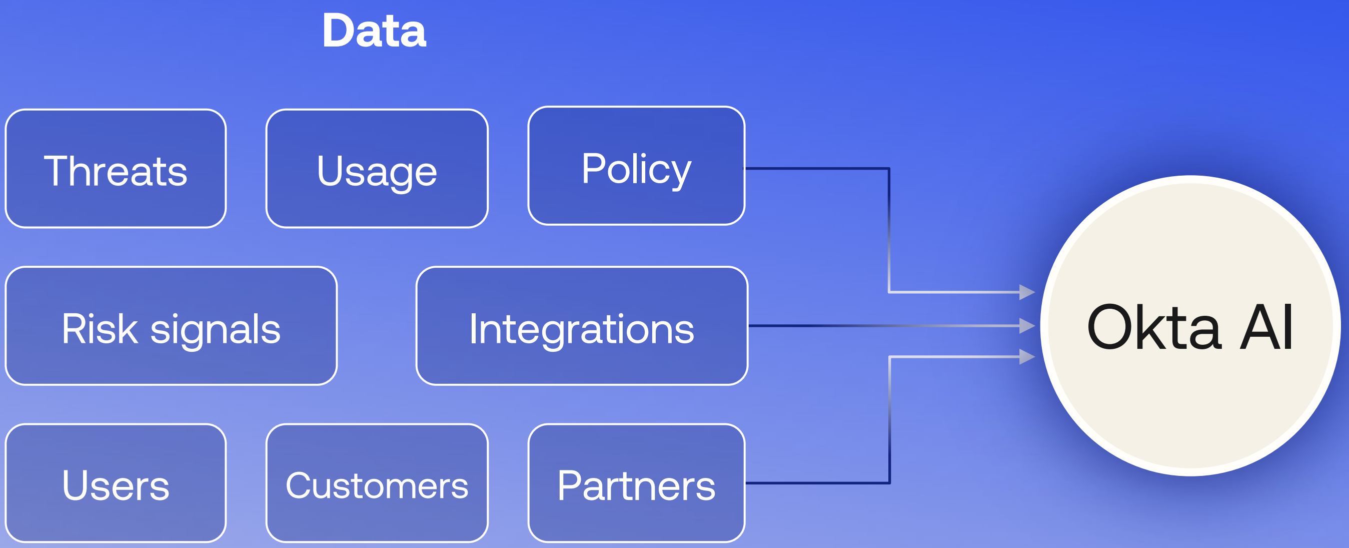
NLP

Features

Deep learning

The evolution of AI





Data

Threats

Usage

Policy

Risk signals

Integrations

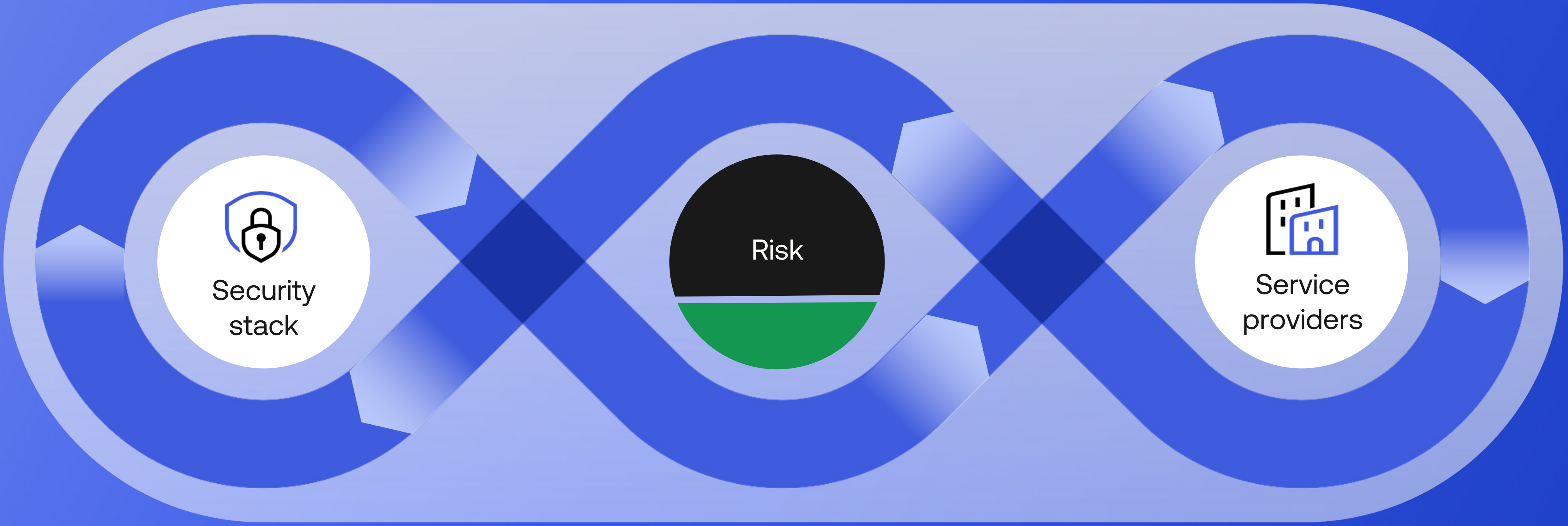
Users

Customers

Partners

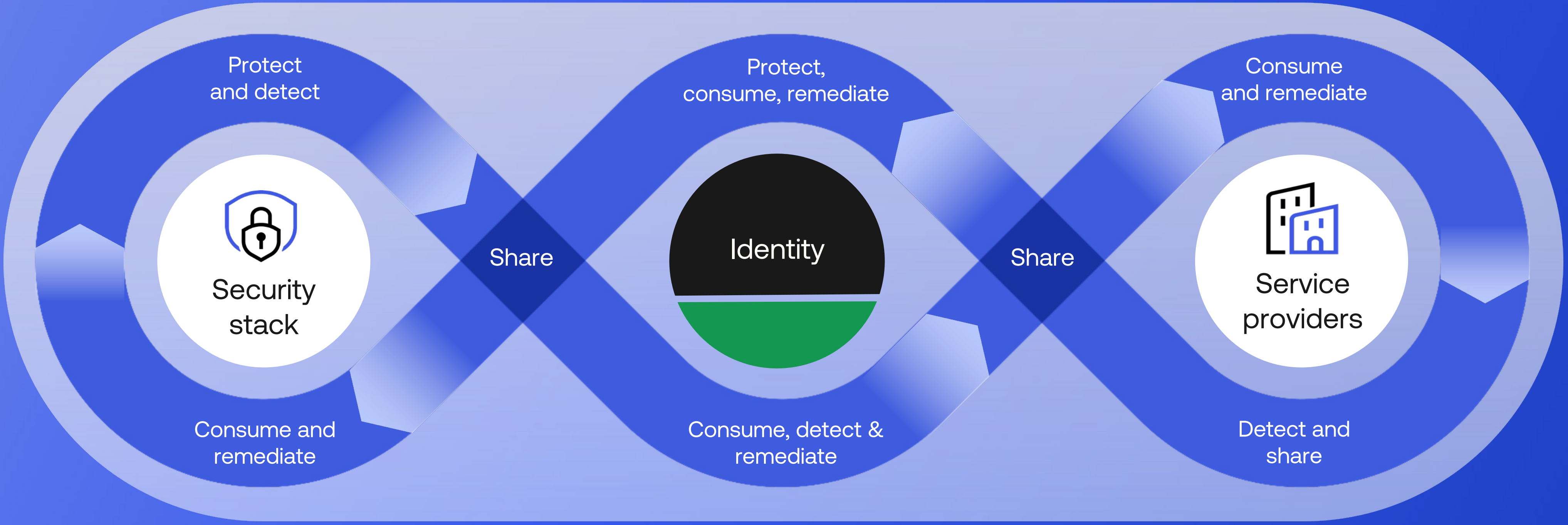
Okta AI

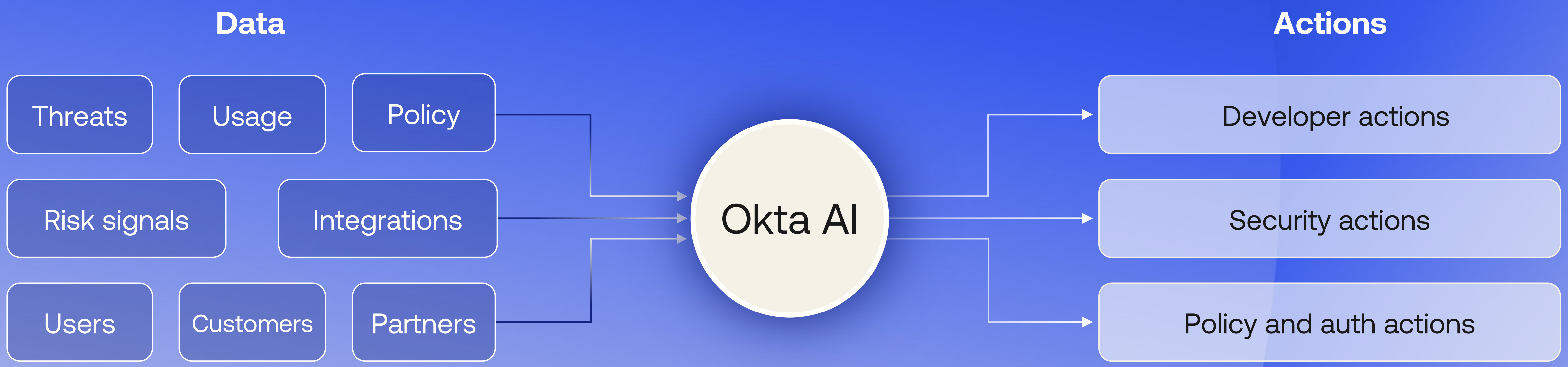
We have no shortage of risk signals, but need the ability to quickly consolidate and take action on those insights



The new security paradigm centralises understanding of risk

A paradigm shift has re-imagined the interaction between IdPs and 3rd-party service providers, with Identity as a central intersection point





Data

- Threats
- Usage
- Policy
- Risk signals
- Integrations
- Users
- Customers
- Partners

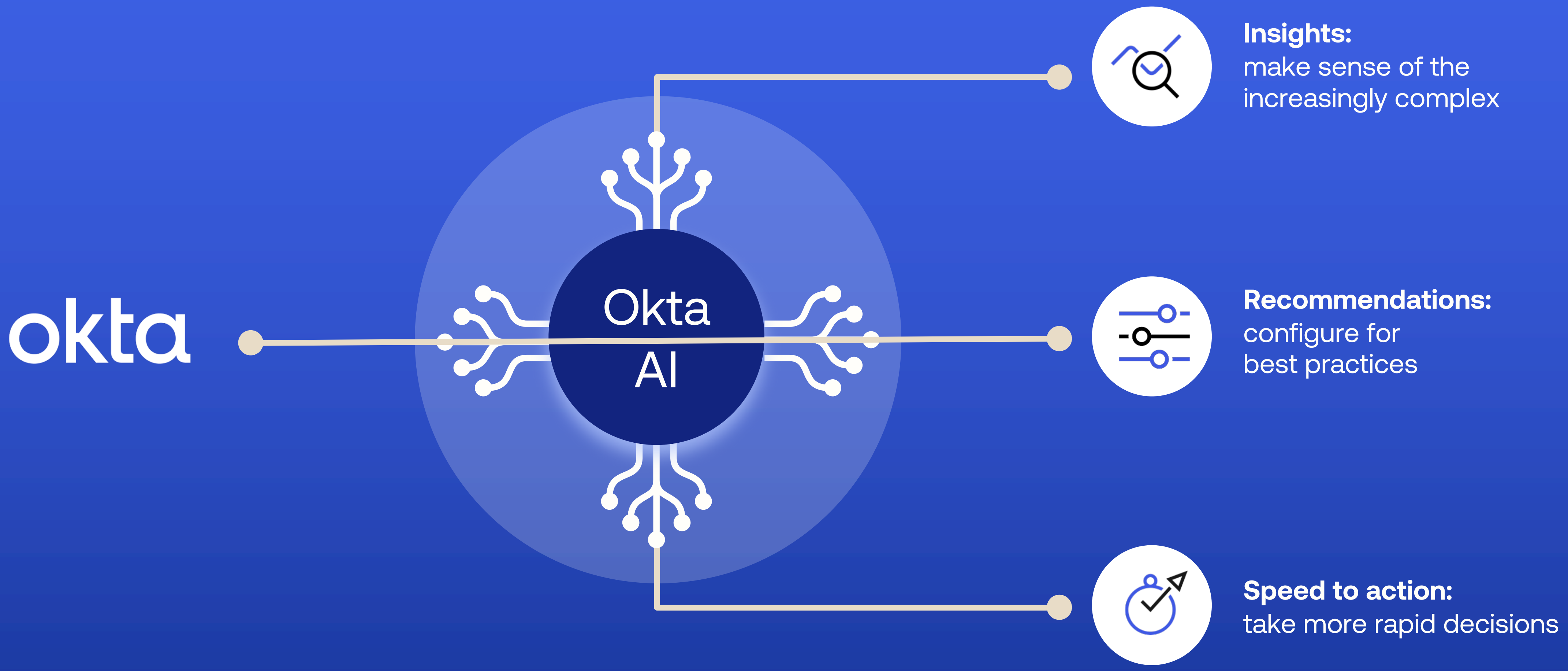
Okta AI

Actions

- Developer actions
- Security actions
- Policy and auth actions

The role of Identity in security

Identity is the connective fabric between the complex ecosystem of people and technologies, securely enabling your workforce to do their best work



Okta AI

Insights:
make sense of the increasingly complex

Recommendations:
configure for best practices

Speed to action:
take more rapid decisions

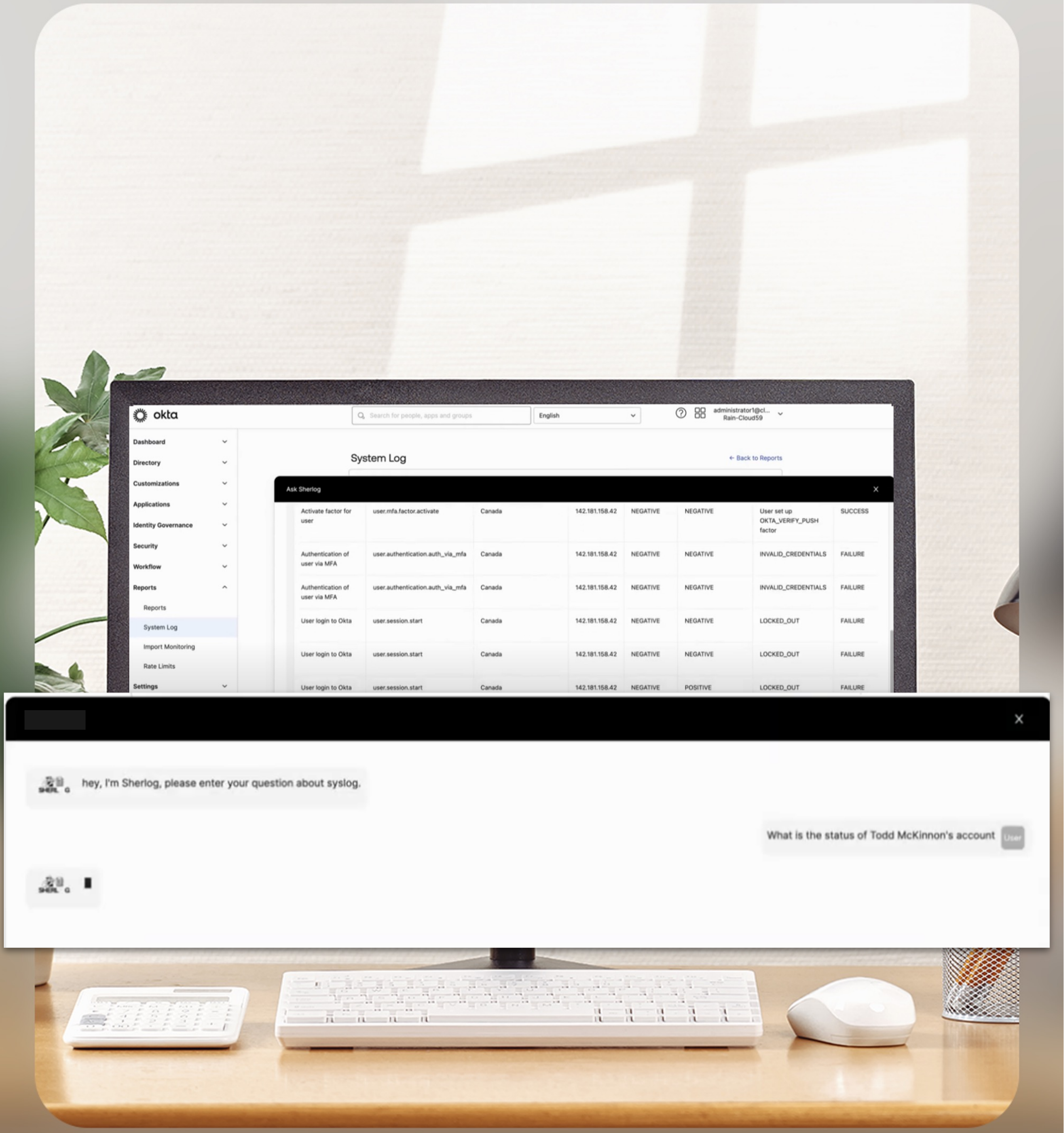
Make sense of the increasingly complex

Log Investigator with Okta AI

Enables admins to ask questions about Okta data in plain English, and obtain insights on the historical context of their Identity posture.

“Have we seen any suspicious logins this week?”

“Who is not using their full G Suite license?”



System Log

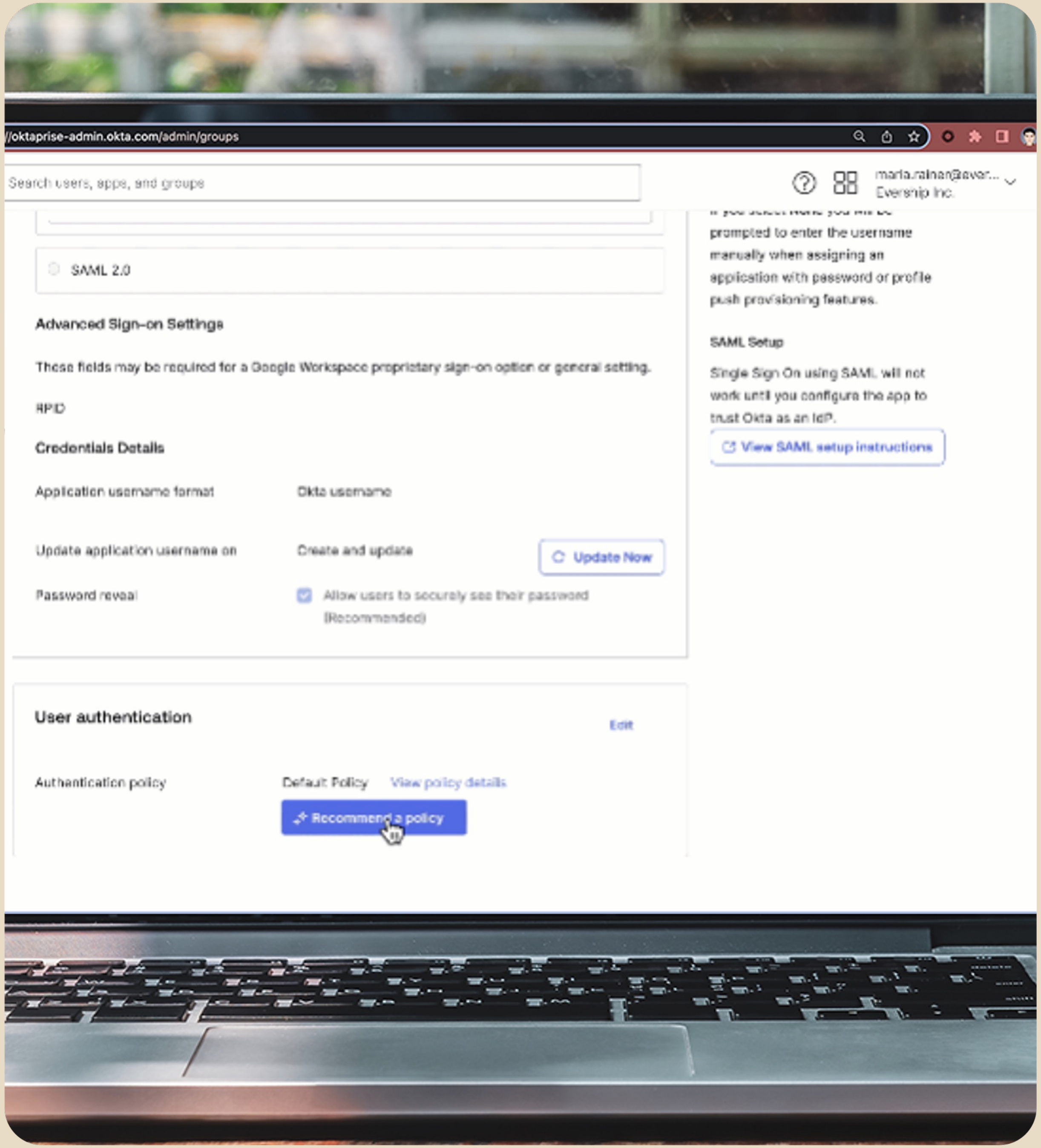
Ask Sherlog

Activate factor for user	user.mfa.factor.activate	Canada	142.181.158.42	NEGATIVE	NEGATIVE	User set up OKTA_VERIFY_PUSH factor	SUCCESS
Authentication of user via MFA	user.authentication.auth_via_mfa	Canada	142.181.158.42	NEGATIVE	NEGATIVE	INVALID_CREDENTIALS	FAILURE
Authentication of user via MFA	user.authentication.auth_via_mfa	Canada	142.181.158.42	NEGATIVE	NEGATIVE	INVALID_CREDENTIALS	FAILURE
User login to Okta	user.session.start	Canada	142.181.158.42	NEGATIVE	NEGATIVE	LOCKED_OUT	FAILURE
User login to Okta	user.session.start	Canada	142.181.158.42	NEGATIVE	NEGATIVE	LOCKED_OUT	FAILURE
User login to Okta	user.session.start	Canada	142.181.158.42	NEGATIVE	POSITIVE	LOCKED_OUT	FAILURE

[redacted]

hey, I'm Sherlog, please enter your question about syslog.

What is the status of Todd McKinnon's account



//oktaprise-admin.okta.com/admin/groups

Search users, apps, and groups

marla.ralnan@ever...
Evership Inc.

○ SAML 2.0

Advanced Sign-on Settings

These fields may be required for a Google Workspace proprietary sign-on option or general setting.

RPID

Credentials Details

Application username format	Okta username	
Update application username on	Create and update	Update Now
Password reveal	☑ Allow users to securely see their password (Recommended)	

If you select None you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

SAML Setup

Single Sign On using SAML will not work until you configure the app to trust Okta as an IdP.

View SAML setup instructions

User authentication Edit

Authentication policy: Default Policy View policy details

Recommend a policy

Configure for best security practices

Policy Recommender with Okta AI

Apply strong security policies with AI-driven insights and recommendations

Aggregated intelligence from across Okta's extensive ecosystem

Recommendations based upon crowdsourced insights as well as best security practices

Optimised security outcomes without overwhelming admins

okta

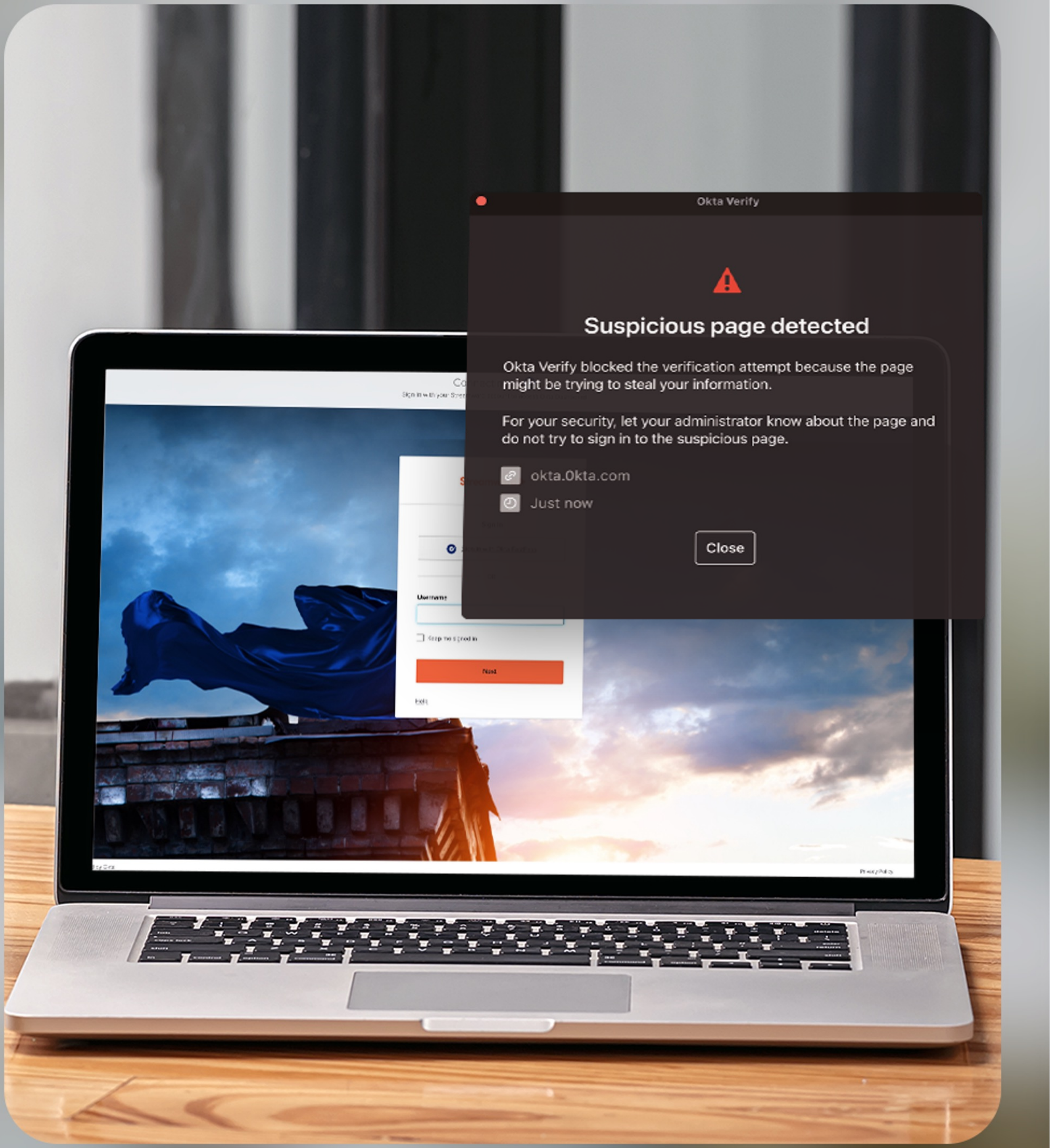
Take more rapid decisions

Identity Threat Protection with Okta AI

Assess identity risk in real-time during login and through active sessions

Amplify threat visibility by harnessing signals from your best-in-breed security ecosystem

Adapt through inline actions and automated workflows to address emerging threats



Suspicious page detected

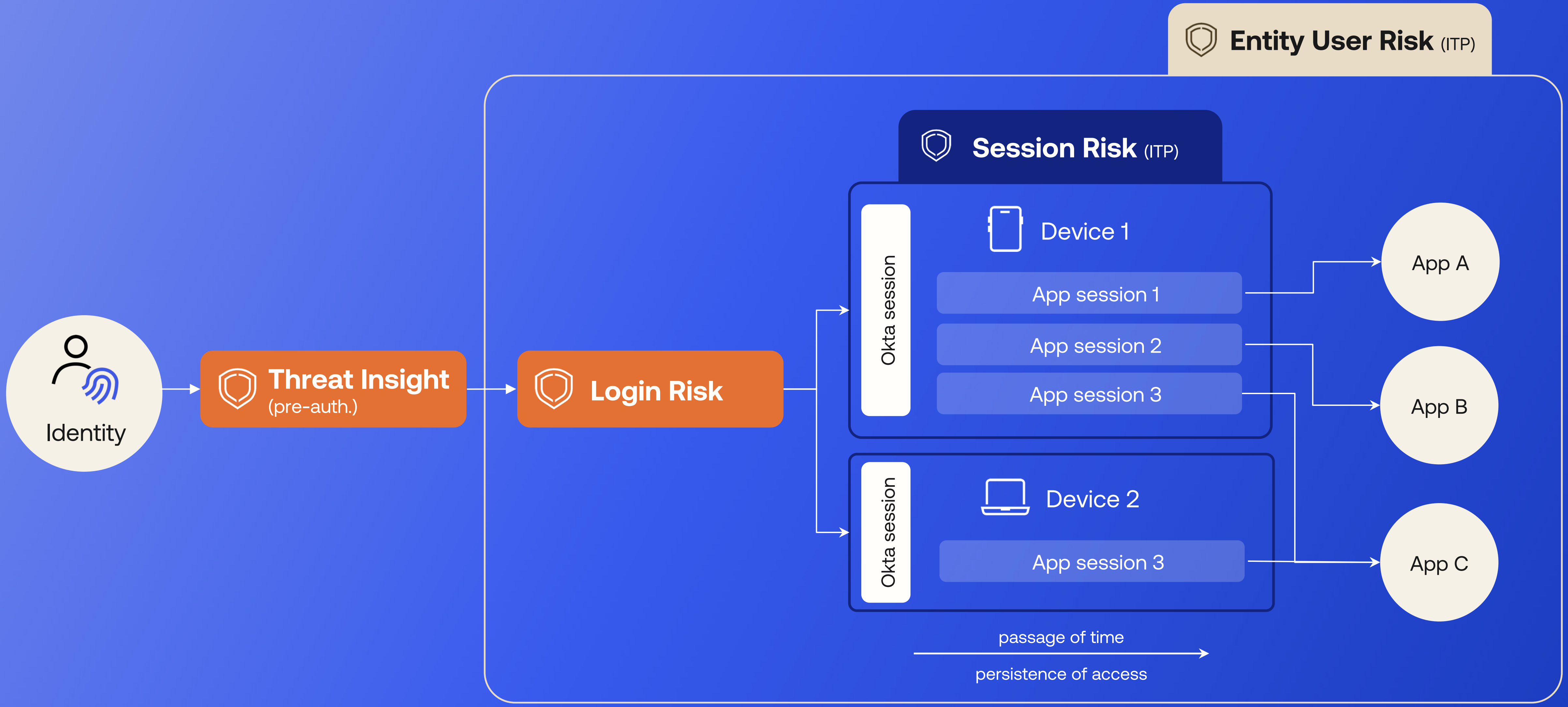
Okta Verify blocked the verification attempt because the page might be trying to steal your information.

For your security, let your administrator know about the page and do not try to sign in to the suspicious page.

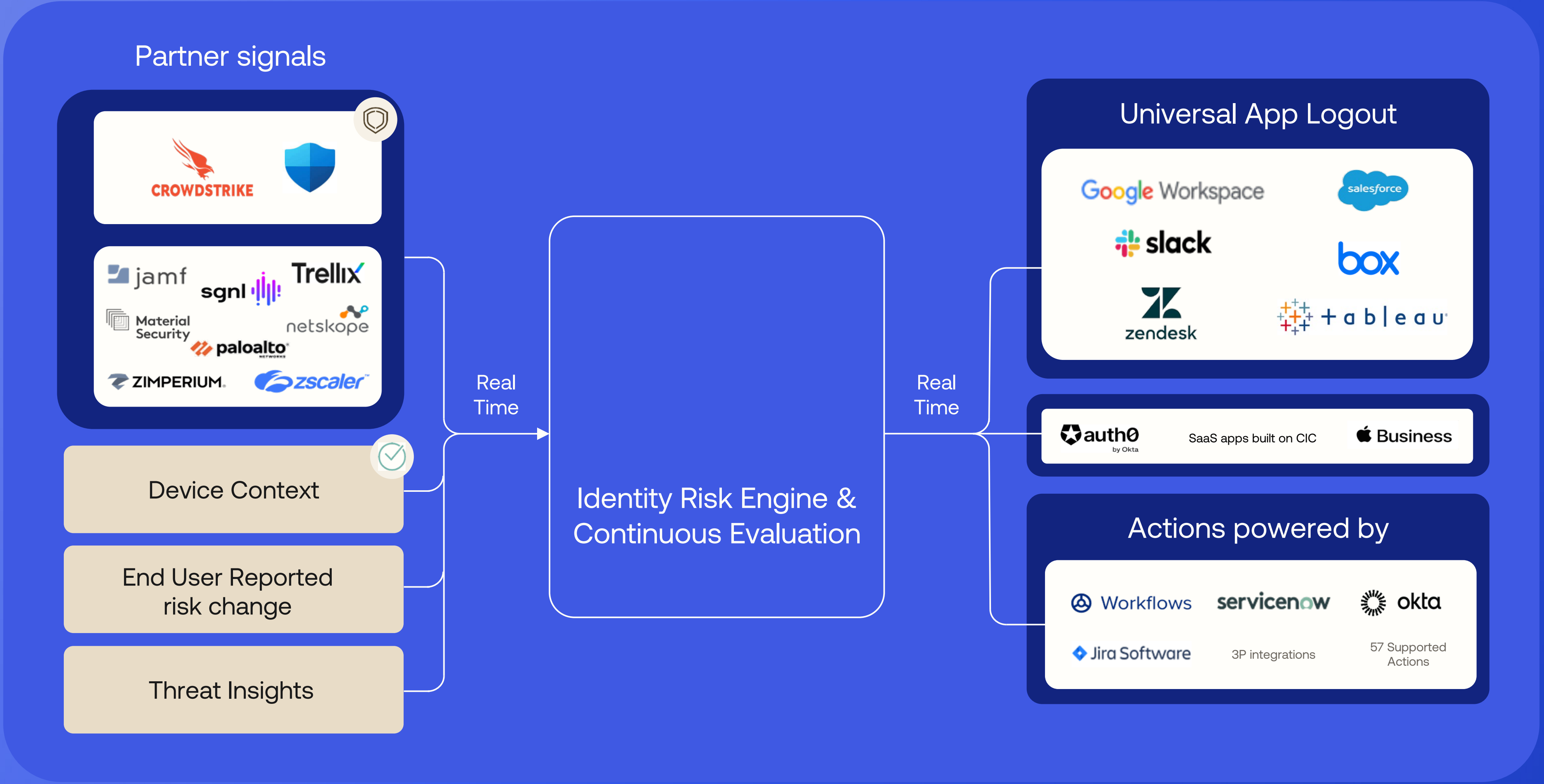
okta.Okta.com

Just now

The new Risk Paradigm: Full 360 Identity Threat Protection



Identity Threat Protection with Okta AI



Partner signals

Device Context

End User Reported risk change

Threat Insights

Real Time

Identity Risk Engine & Continuous Evaluation

Real Time

Universal App Logout

SaaS apps built on CIC

Actions powered by

3P integrations

57 Supported Actions

With the power of new AI models comes greater responsibility

The attackers are already using AI, so should you

You can too for:

Insights:
Make sense of the increasingly complex

Recommendations:
Configure for best security practices

Speed to action:
Take more rapid decisions

Continue the conversation at **Booth 629**

Thank You