okta
The World's Identity Company

SINC

The Power of Identity

Gaurav Ranjit, Sr CSM

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.

okta

Speaker

Gaurav Ranjit

Sr Customer Success Manager

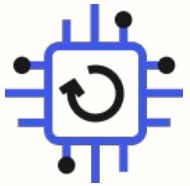
- 15+ years of experience in the IAM industry
- Primary customer focus is C-Suite management
- Passionate about emerging technologies & its application
- An avid travel enthusiast & blogger

LinkedIn: https://www.linkedin.com/in/gauravranjit/

Goal of Today's Presentation

Embracing Zero Trust

Importance of Identity in Threat Protection



Future of Identity with AI

Key Industry Observations

84%

CIO’s want to use GenAI to support new business models

63%

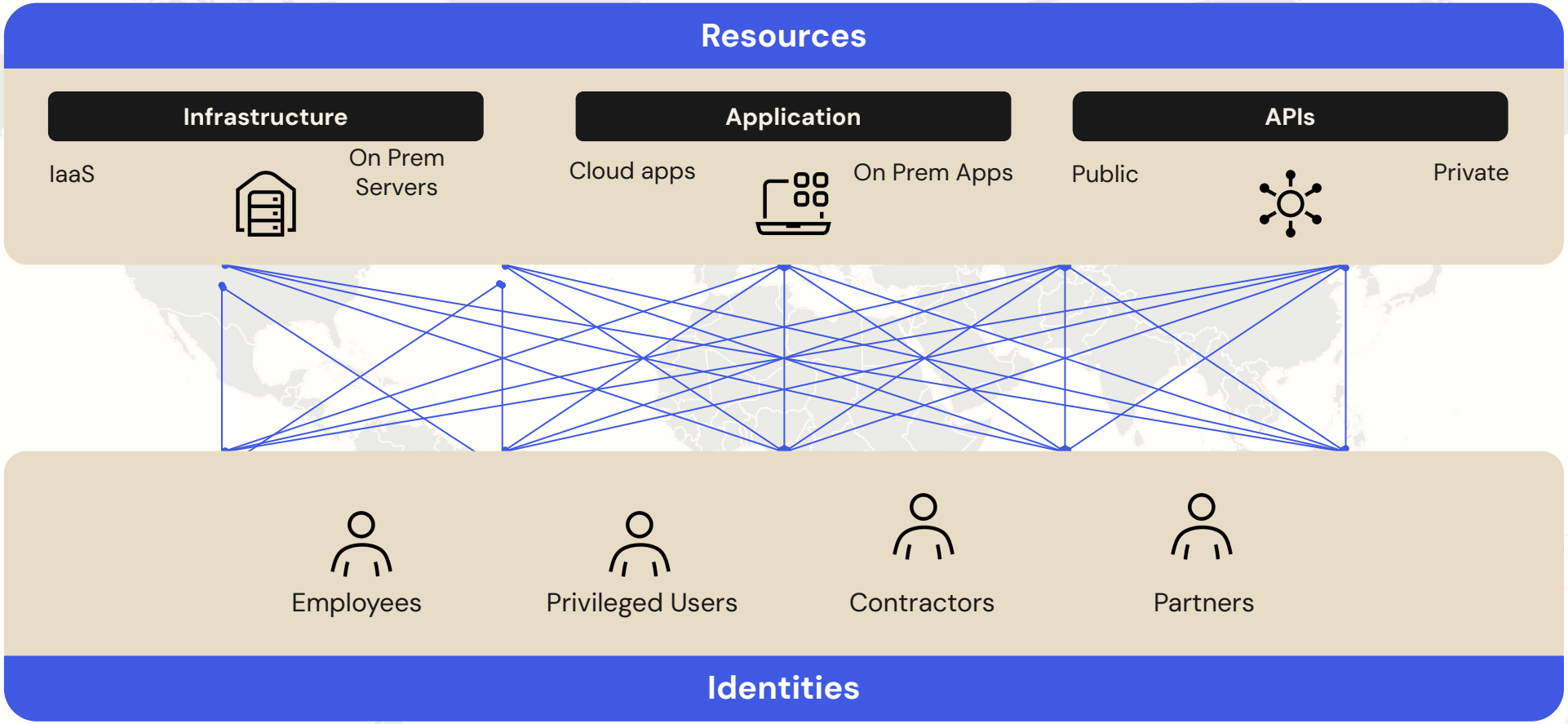
Executives have to say their company's loyalty program budget increased in the latest planning cycle

25%

Organizations are incorporating data security and privacy features into applications, products, services and third-party relationships

Source: *https://www.pwc.com/us/en/executive-leadership-hub*

Enterprise Tech is getting more and more complex...



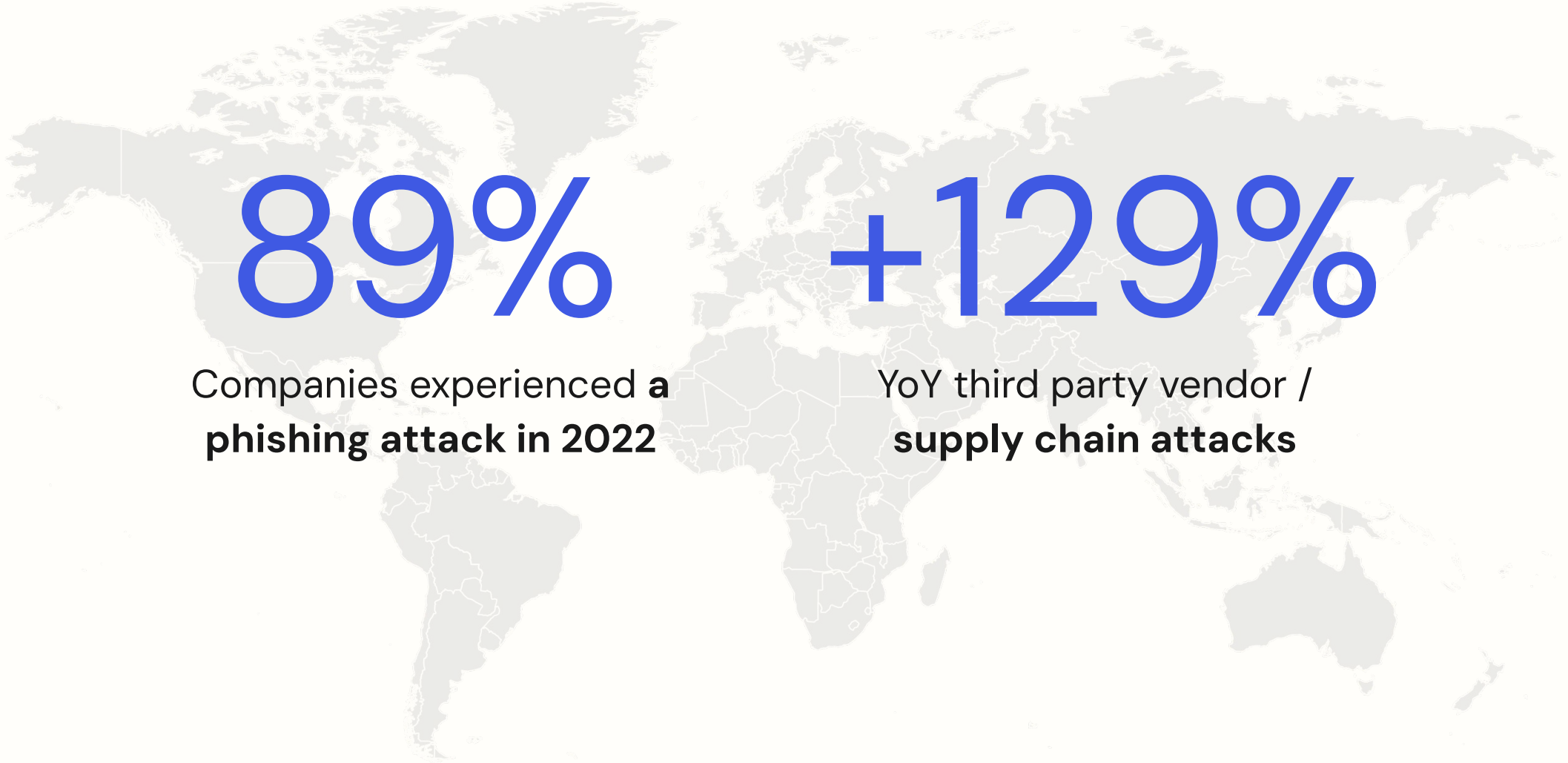
IT + Security need to do more with less...

okta

Our vision

Free everyone to safely use any technology

And the threat landscape revolves around Identity



89%

Companies experienced **a phishing attack in 2022**

+129%

YoY third party vendor / **supply chain attacks**

okta

Embracing Zero Trust

Setting the Stage

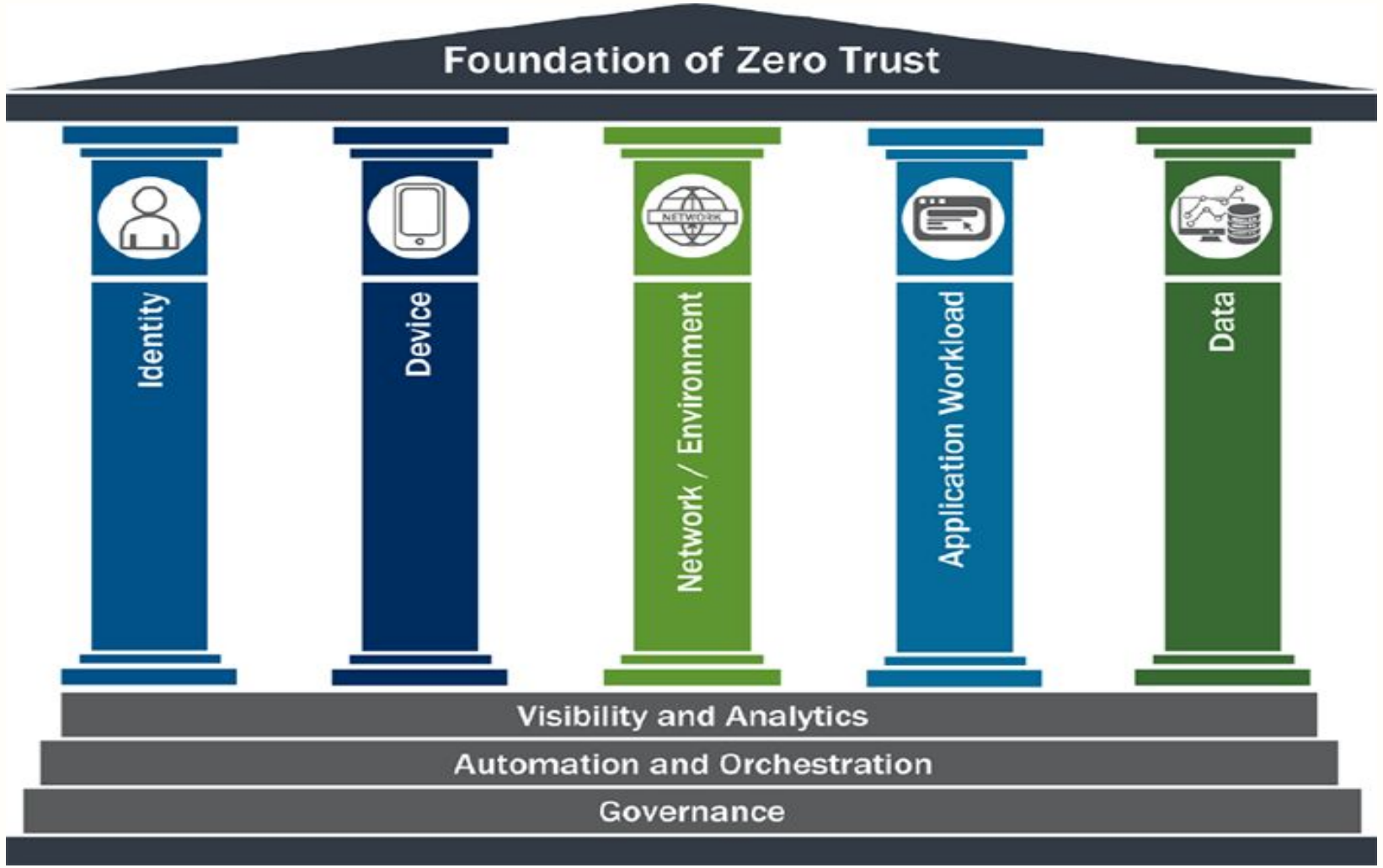
Embracing Zero Trust

Convergence of Security & Identity

The Future of Identity with AI

Summary & Conclusion

CISA Zero Trust Model

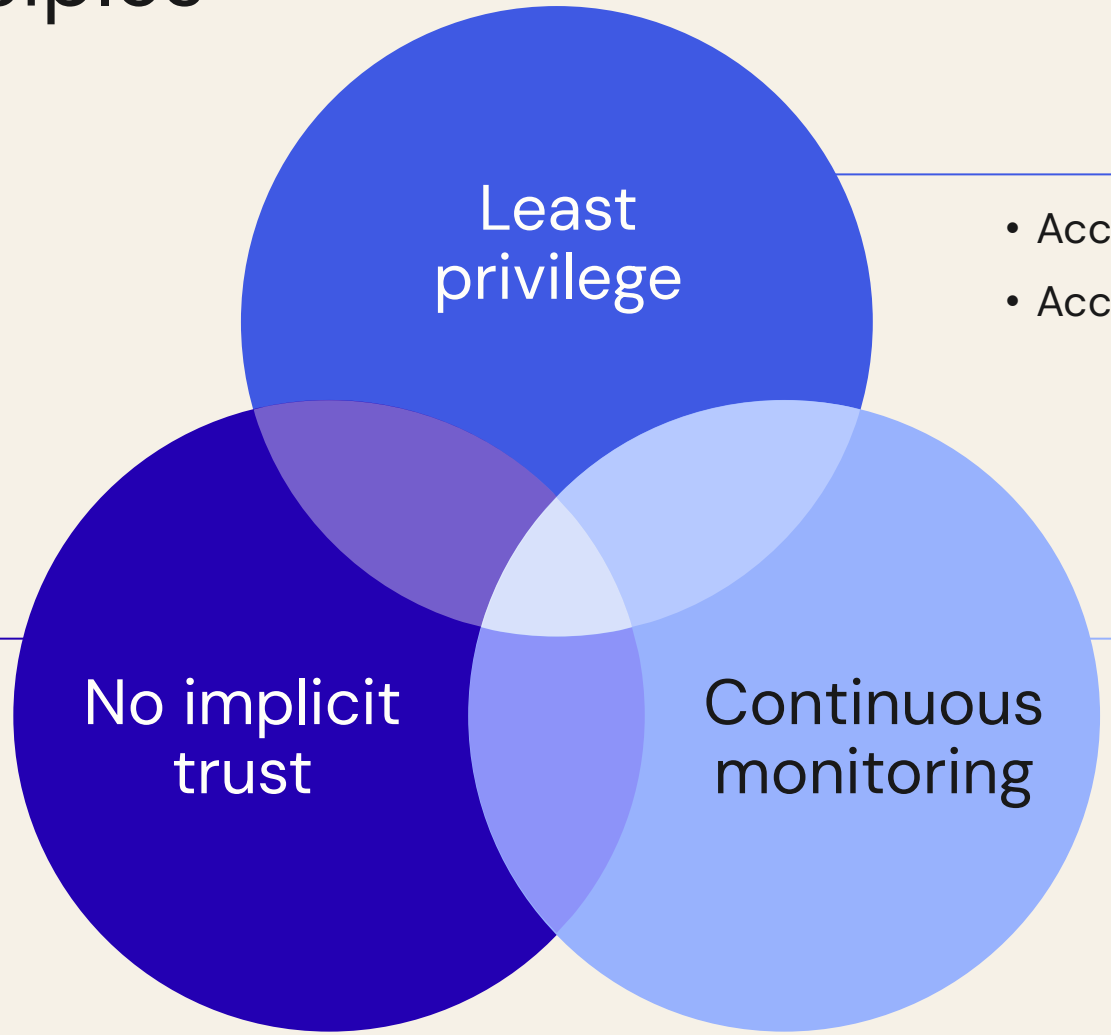


Core Principles

- Least Privilege
- No Implicit Trust
- Continuous Monitoring

okta

Zero Trust Principles



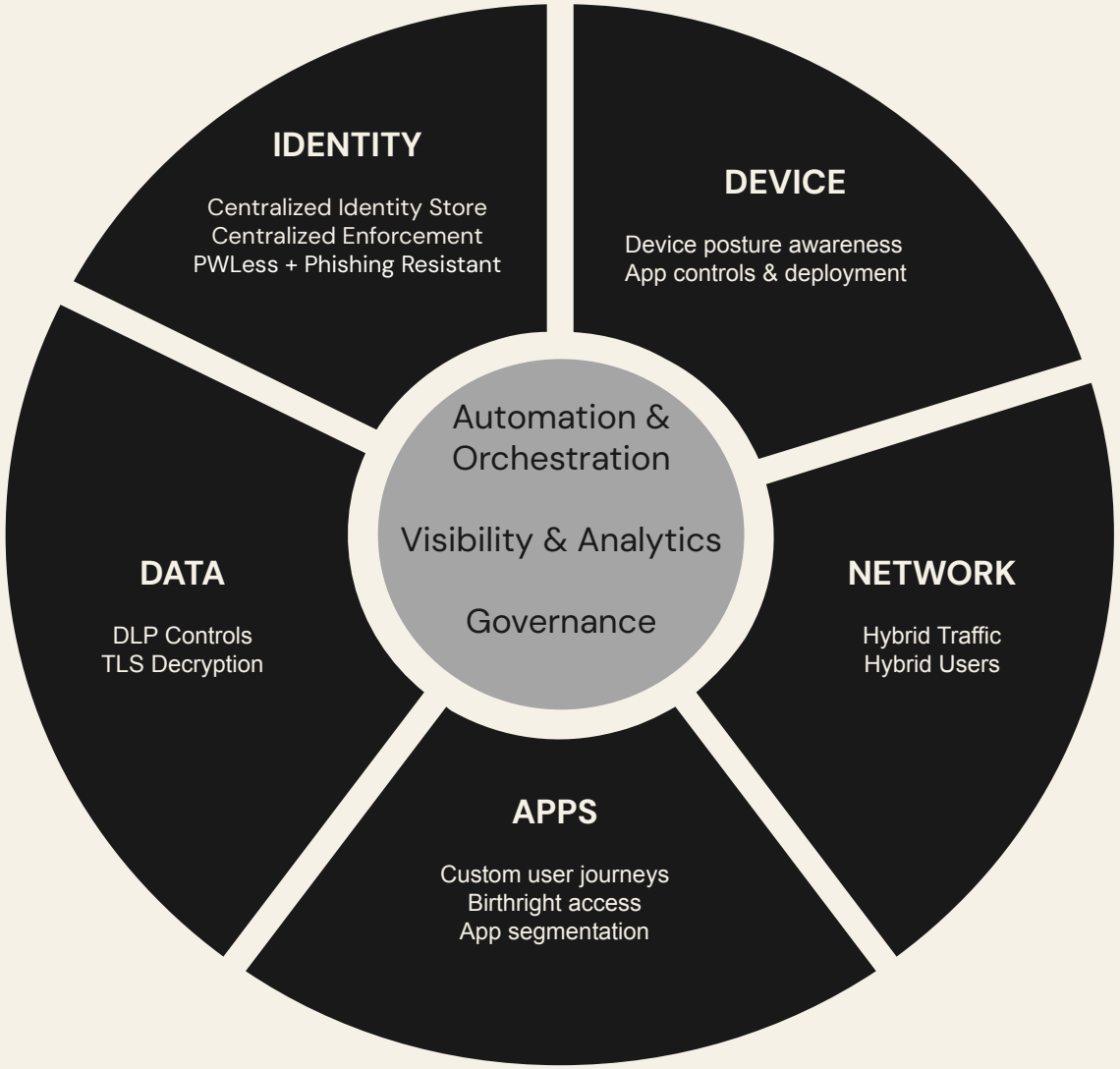
- Access granted per session
- Access granted per resource

- Policy driven AuthN & AuthZ
- Integrity and security of assets
- Secure communication

- Continuous enforcement
- Dynamic observable state

okta

How Zero aligns to Organizational Business Drivers



Security Projects

- Security Tool Consolidation
- Reduce Identity Breaches
- Protect against data exfil
- BYOD Offering
- Granular Policy Enforcement

Business Projects

- M&A efforts
- Expanded Workforce (B2B/Contractors)
- Increased Productivity
- Improved UX
- Cloud Migration
- Compliance

Business Value

- Operational Efficiency
- Cost Savings
- Cyber Resilience
- Reduce cost of breaches
- Pursue Compliance
- Increased market confidence

okta

Three foundational elements to begin your Zero Trust journey

Identities

Endpoints

Applications

Only **trusted devices** and **trusted users** should be allowed access to **authorized applications**

okta

The Convergence of Security & Identity

Setting the Stage

Embracing Zero Trust

Convergence of Security & Identity

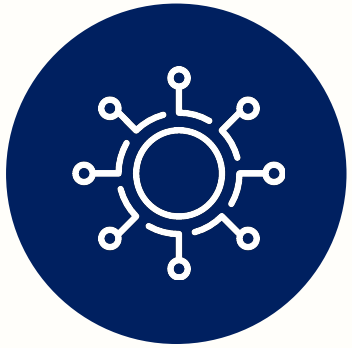
The Future of Identity with AI

Summary & Conclusion

New and existing threats pose different challenges

Evolving threat landscape

Threats have become more sophisticated and are increasing in number



Expanded attack surface

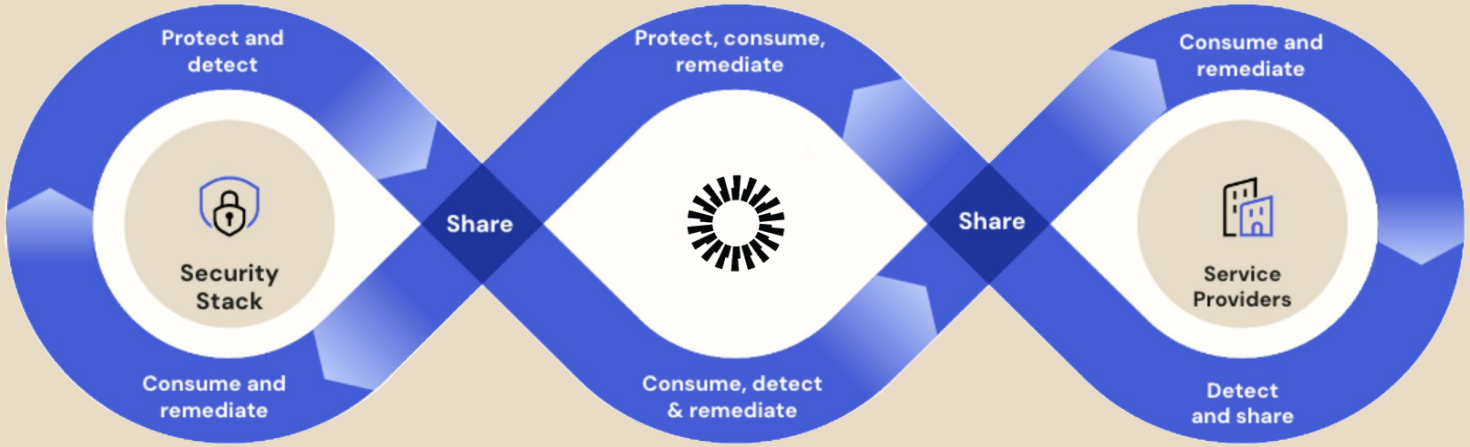
Identities, endpoints, applications, and networks are main attack vectors, especially with a distributed workforce

Siloed and complex security stacks

Hidden risks and visibility gaps with point security solutions that don't integrate with each other provide a false sense of security

okta

Taking the Centered Approach



Shared Signals Pipeline

Ingest third-party risk signals across the security stack

Risk Engine

Continuously evaluates login, session, and entity risk with AI-powered threat detection.

Adaptive Actions

Configurable real-time responses to threats based on risk level, such as **Universal Logout**

okta

Okta Identity Cloud

A unified and neutral solution for everyone and every identity need

POSTURE ENFORCEMENT + OBSERVABILITY (Spera Security)

OKTA INTEGRATION NETWORK | Connect everything

Access Management

Any resource. Any device. Anywhere.
One secure passwordless experience.

Identity Governance

The right level of access, from a user's first day to their last.

Privileged Access

Least privilege for everything. No matter who they are, or what device they use.

PLATFORM | 99.99% Uptime

Directories
Connect in and manage all of your people

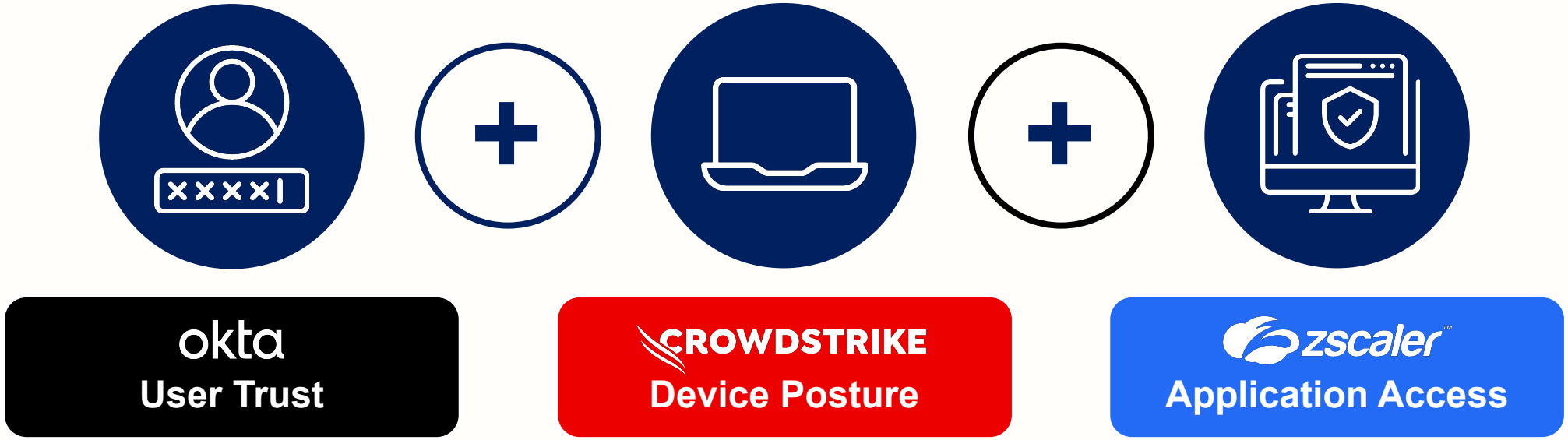
AI, Insights, Reporting
All the data

Extensibility
Pro code or no code tools across Okta APIs + SDKs

Risk Signals
Connect in signals across your stack

Employees | Contractors | Business Partners

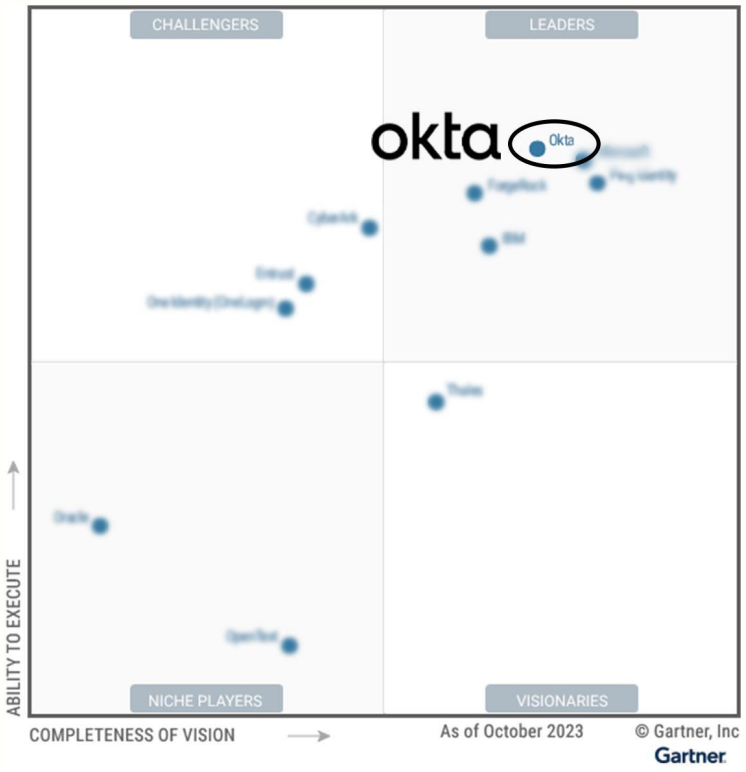
Security Starts with Identity



Integrated to share telemetry and threat intelligence and trigger cross-platform response

Recognized as leaders by trusted analyst firm

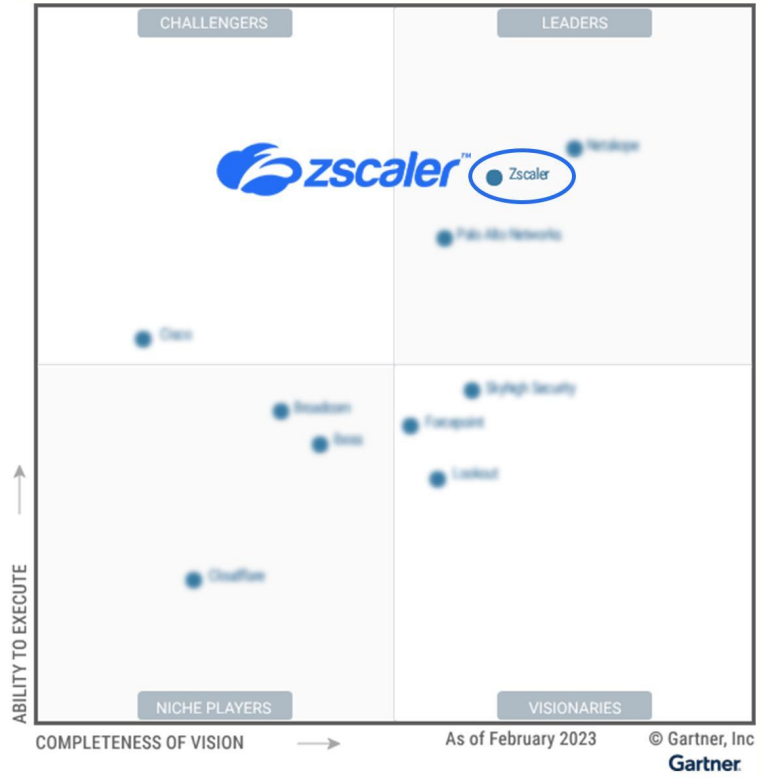
Gartner® Magic Quadrant™ for:



Access Management

Source: Gartner (December 2022)

Endpoint Protection Platforms



Security Service Edge

okta

Key business outcomes

Prevention

Reduce the attack surface and prevent compromise through threat intel and cross-domain telemetry sharing to drive Zero Trust access control decisions

Containment

Provide real-time threat containment by preventing lateral movement with threat detection and enabling cross-domain enforcement

Response

Accelerate multi-domain response through contextual telemetry sharing to triage incidents, leading to faster and more precise remediation

okta

Future of Identity with AI

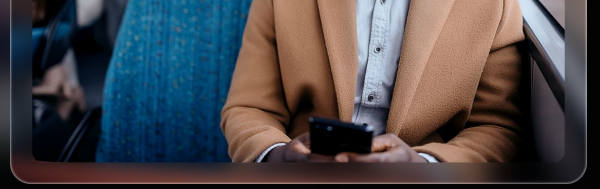
Setting the Stage

Embracing Zero Trust

Convergence of Security & Identity

The Future of Identity with AI

Summary & Conclusion

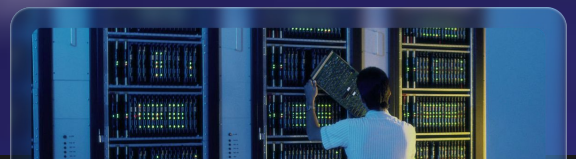


Mainframe

Personal computing

Client-server

Internet



Every company is an AI company

Every company is a technology company

> "By 2025 at least 35% of organizations will utilize generative AI as part of their identity fabric functions. These organizations 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

Organizations

Proactive security

Customers

Frictionless user experience

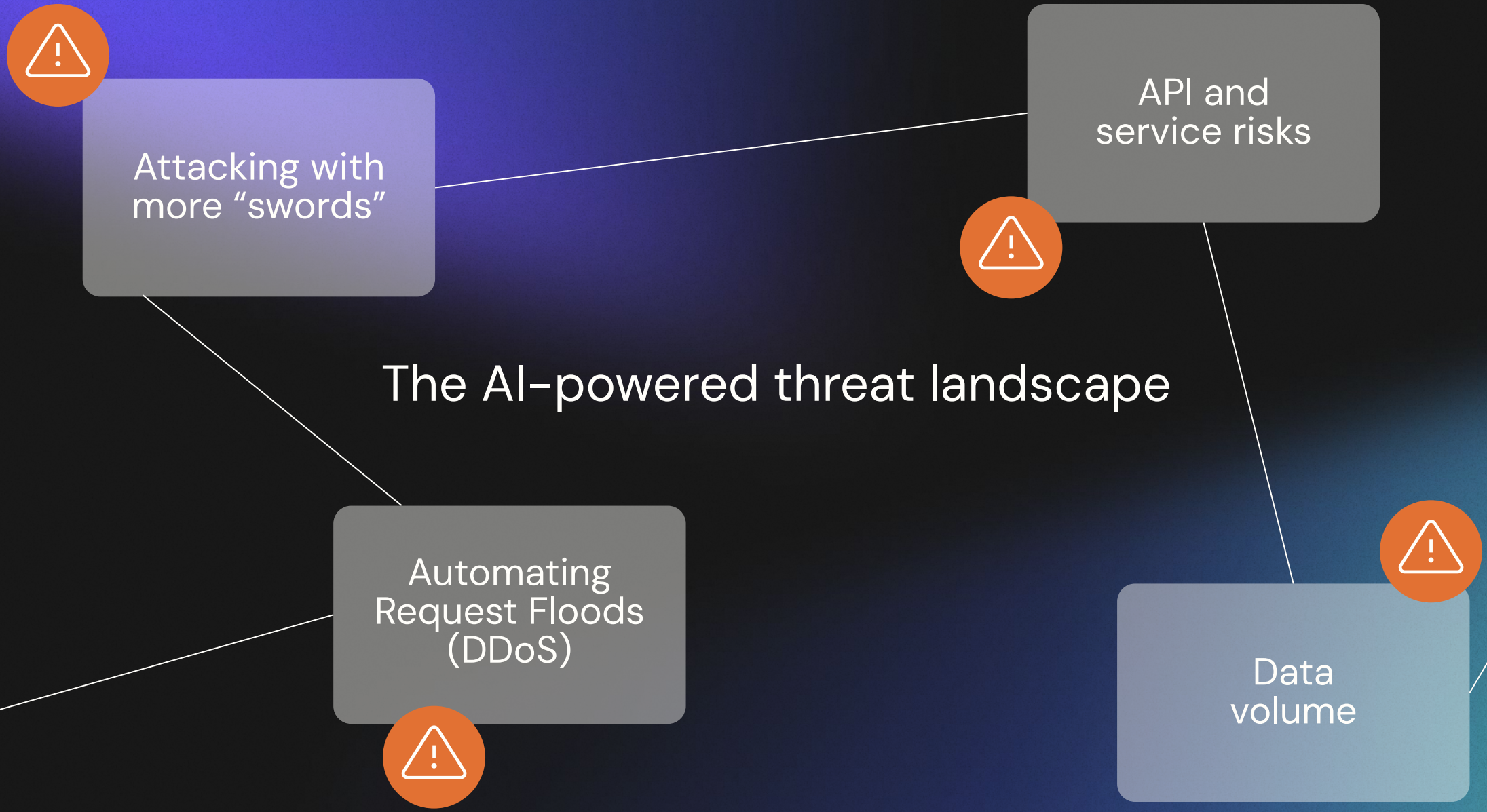
Developers

Build apps faster

Extended workforce

Efficient workflow automation

The AI-powered threat landscape



oktane

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

ChatGPT

Machine Learning

Predictive Analysis

Optimization

Data Science

Computer Vision

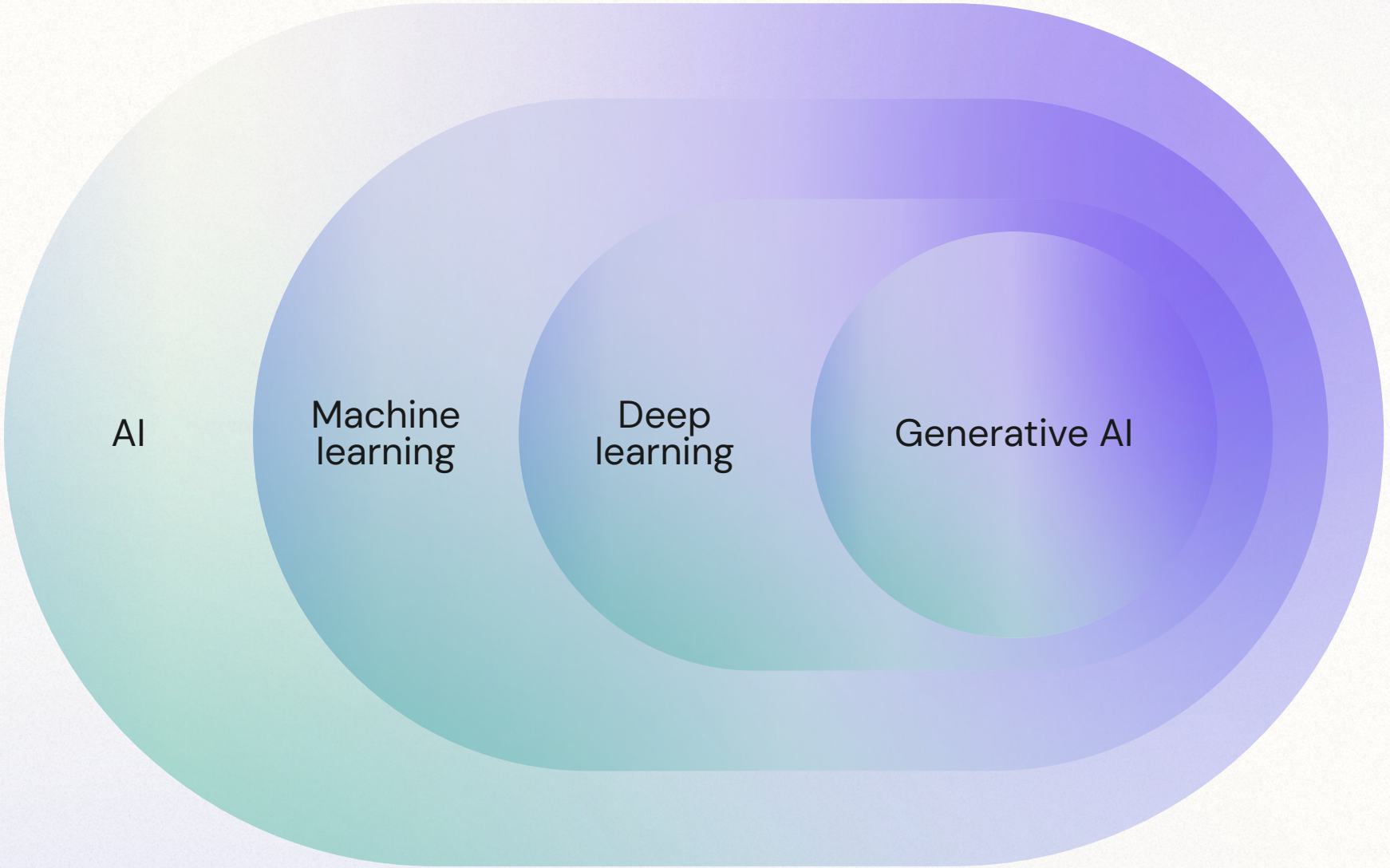
Data Mining

Deep Learning

Features

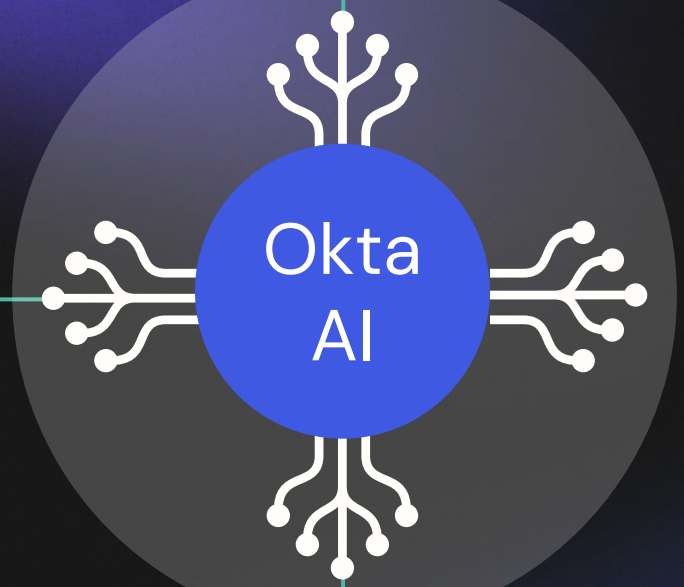
NLP

oktane



The evolution of AI.

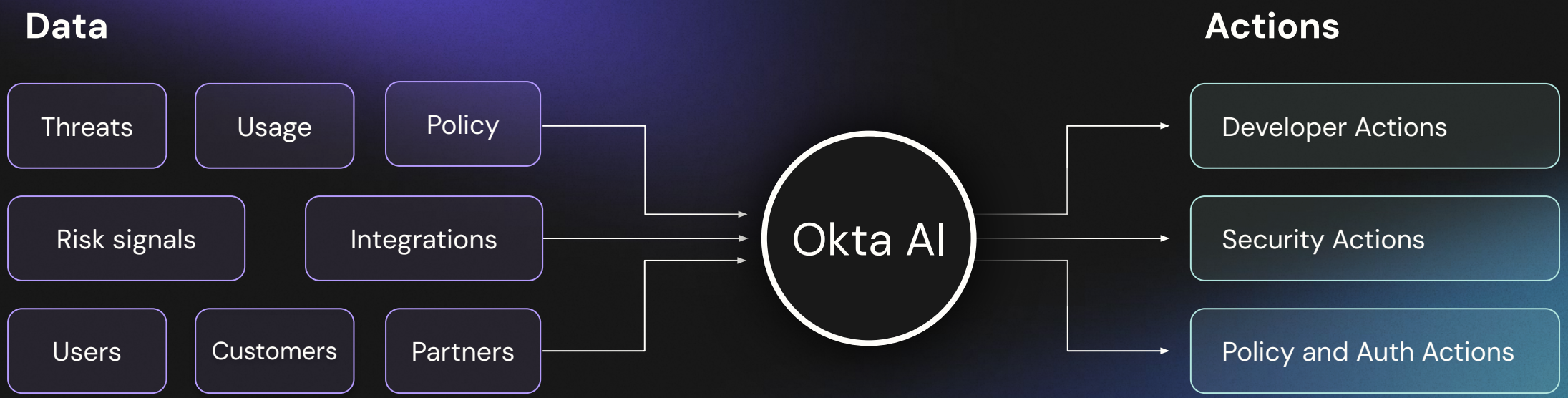
okta



Security:
Prevent, detect, recover, and remediate increasingly sophisticated attacks

Efficiency:
Faster+better decisions, reducing IAM complexity, lowering cost through automation

okta



In Conclusion

Setting the Stage

Embracing Zero Trust

Convergence of Security & Identity

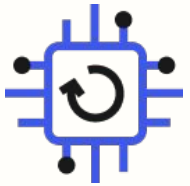
The Future of Identity with AI

Summary & Conclusion

Conclusion

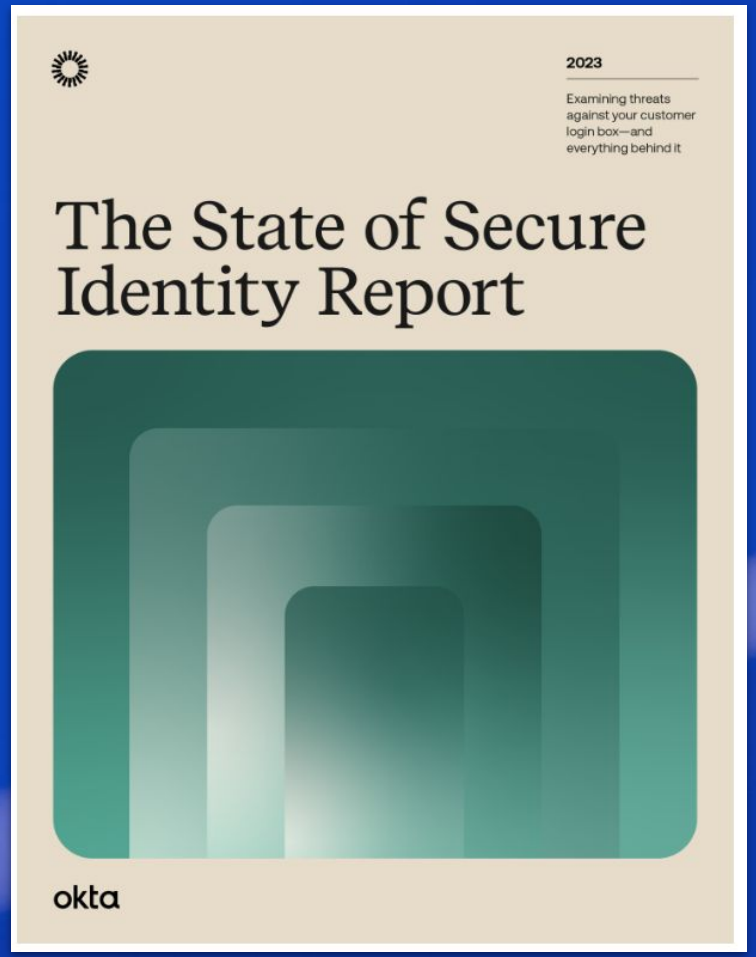
Zero Trust is Foundational to Strong Security Culture

Break the silos in security & approach it with an identity centric lens



AI is the future, and Identity plays a critical role

Thank you!



Link to the Report

Link to the Report

okta

The World's Identity Company