tanum consult
Information Security

okta

Reduce Risk with Okta's End-to-End Unified Identity Platform

5. Juni 2025, München

Renold Gehrke
Senior Regional Alliances Manager
renold.gehrke@okta.com

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, business strategy and plans, market trends and market size, opportunities and positioning. 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, global economic conditions have in the past and could in the future reduce demand for our products; we and our third-party service providers have in the past and could in the future experience cybersecurity incidents; we may be unable to manage or sustain the level of growth that our business has experienced in prior periods; our financial resources may not be sufficient to maintain or improve our competitive position; we may be unable to attract new customers, or retain or sell additional products to existing customers; customer growth has slowed in recent periods and could continue to decelerate in the future; we could experience interruptions or performance problems associated with our technology, including a service outage; we and our third-party service providers have failed, or were perceived as having failed, to fully comply with various privacy and security provisions to which we are subject, and similar incidents could occur in the future; we may not achieve expected synergies and efficiencies of operations from recent acquisitions or business combinations, and we may not be able to successfully integrate the companies we acquire; 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 products, features, functionalities, certifications, authorizations, or attestations referenced in this presentation that are not currently generally available or have not yet been obtained or are not currently maintained may not be delivered or obtained on time or at all. Product roadmaps do not represent a commitment, obligation or promise to deliver any product, feature, functionality, certification or attestation and you should not rely on them to make your purchase decisions.

okta

Okta at a glance

Founded in San Francisco

2009

6,000+

Employees worldwide

20,000+

Active customers

In CEE

2019

7,600+

Okta Integrations

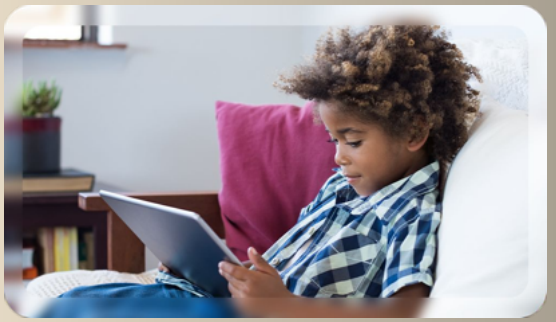
$469mio+

Investestment into R&D

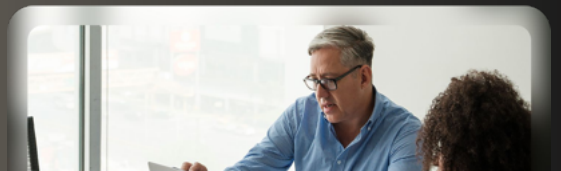
okta

Identity is Security

okta



If you were breached right now, how long would it take for you to detect it?



mation of Okta –

Today's Threat Landscape

292

Days

Average to identify and contain a breach[1]

180%

3x Increase

Breach volume from previous year[2]

3 of 4

Breaches

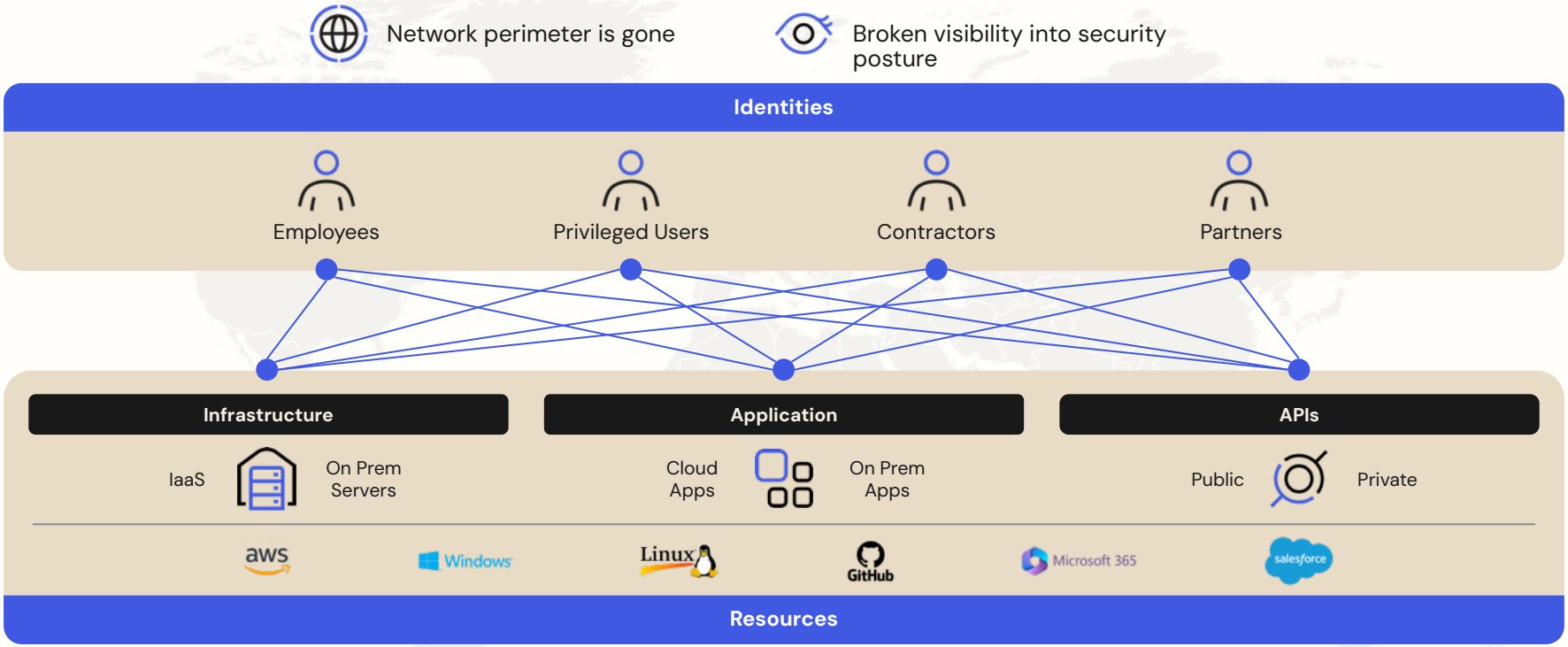
Are Identity-Based[3]

[1] IBM Cost of a Breach Report 2024

[2] 2024 Verizon Data Breach Investigations Report

[3] 2024 Verizon Data Breach Investigations Report

Cloud explosion is making security more complex



okta

The need for an end-to-end unified security solution

Authentication

BEFORE

Discover & Determine

DISCOVER
critical roles, resources, misconfigurations

- ✓ Identity Security Posture Management (ISPM)

DETERMINE
least privilege access controls, strong access policies, risk-based response policies

- ✓ Okta Identity Governance (OIG)
- ✓ Okta Privileged Access (OPA)
- ✓ Life Cycle Management (LCM)

DURING

Enforce

ENFORCE
phishing-resistant, biometric access policies across critical roles + resources

- ✓ Okta Access Management
  - Adaptive MFA
  - Single Sign-On (SSO)
  - API Access Management

AFTER

Detect & Respond

DETECT
and evaluate threats across security tooling

- ✓ Identity Threat Protection (ITP)

RESPOND
with risk-based automation across users, applications, and devices

- ✓ Okta Identity Governance (OIG)
- ✓ Identity Threat Protection (ITP)

Orchestration drives powerful enterprise-wide security outcomes

Secure identity before, during, and after authentication

- ➔ Centralize management, determine least privilege access controls
- ➔ Enforce phishing-resistant authentication policies across all resources
- ➔ Standardize threat response and orchestration

Harden corporate infrastructure by protecting non-human identities

- ➔ Discover risky service accounts
- ➔ Federate, vault & centrally manage service accounts
- ➔ Automatically remediate critical risks

Integration risk reduction and efficiency during mergers and acquisitions

- ➔ Conduct pre-integration security reviews
- ➔ Day 1 access to critical resources and enforcement of security policies
- ➔ Continually monitor and assess risk

A Path to a New Identity Security Standard

OpenID Foundation's Interoperability Profiling for Secure Identity in the Enterprise (IPSIE) Working Group

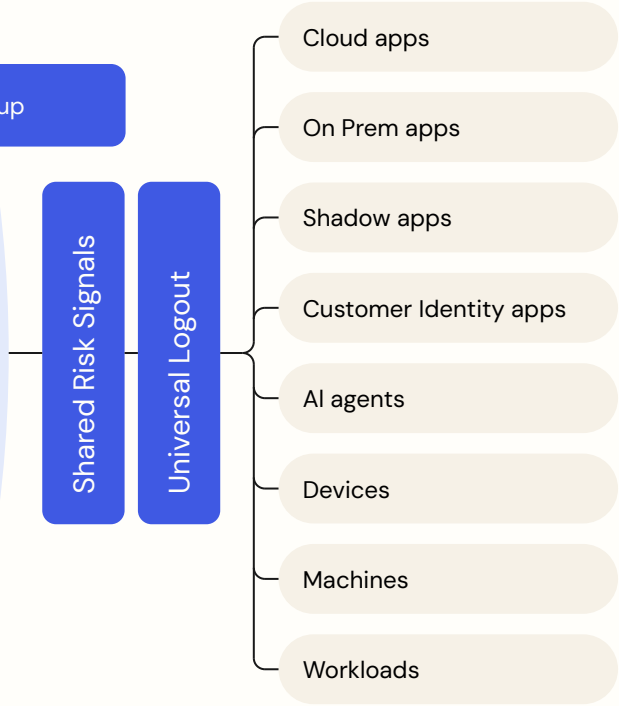
SSO/ MFA

Lifecycle management

Entitlements

Risk signal sharing

Session termination



okta

The ONLY Identity Security Fabric you'll ever need

Secure Identity Products

Posture Management	Governance	PAM	Access Management	Device Access	Identity Threat Protection
Okta Identity Governance	Identity Security Posture Management	Okta Privileged Access	Universal Directory Single Sign-On Adaptive MFA API Access Management Okta Access Gateway Customer Identity	Okta Device Access	Okta Identity Threat Protections

Secure Identity Orchestration

Secure Identity Integrations

Infrastructure	Applications	APIs	Identities
IaaS  On Prem Servers	Cloud Apps  On Prem Apps	Public  Private	Directories  Non Human / AI Agents

99.99% Uptime. Tens of Billions of Monthly Logins. Zero Planned Downtime.

Okta Identity Governance

Access request
Approvals informed by Universal Directory
Auto provisioning
Audit reporting

Access Certification
Informed by authentication data
Governance policies
Audit reporting

Identity Lifecycle Management
Directory sync and HRaaS
Identity lifecycle synced across Authn + Givernance
Provisioning/ deprovisioning

Workflows
Extensibility
Low code/No code Platform

Entitlement Management
BYO entitlements
Fine-grained access
Attribute-based policies

okta

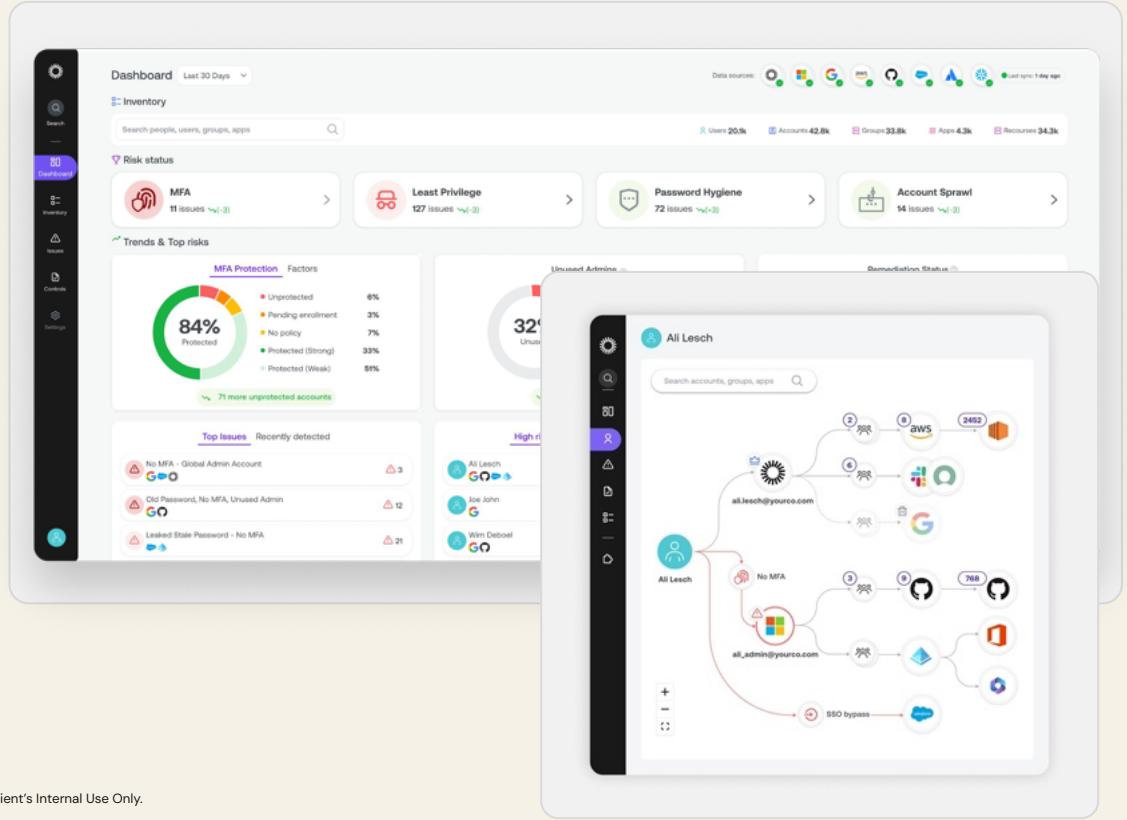
Identify your biggest identity security risks with Identity Security Posture Management (ISPM)

Deep Identity-focused posture analysis

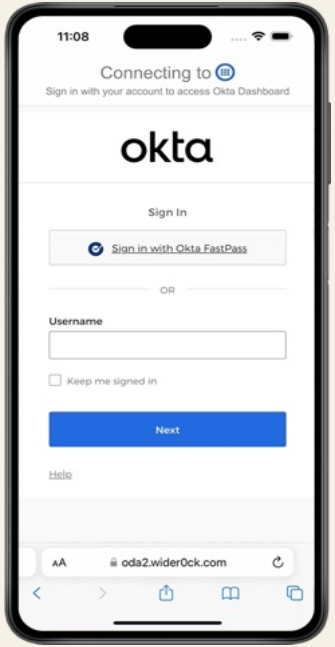
Prioritized with end-to-end context

Continuous validation mapped to common frameworks

Integrated Remediation Workflows

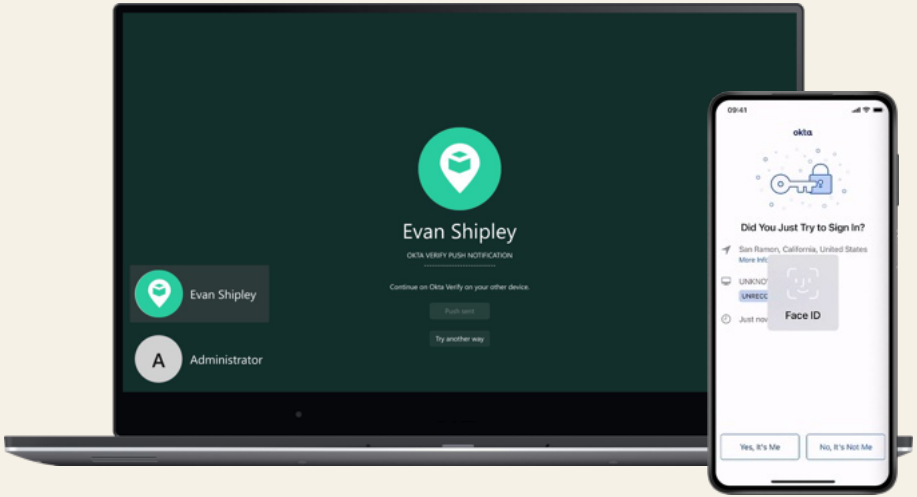


FastPass delivers defense in depth and breadth across all apps and devices

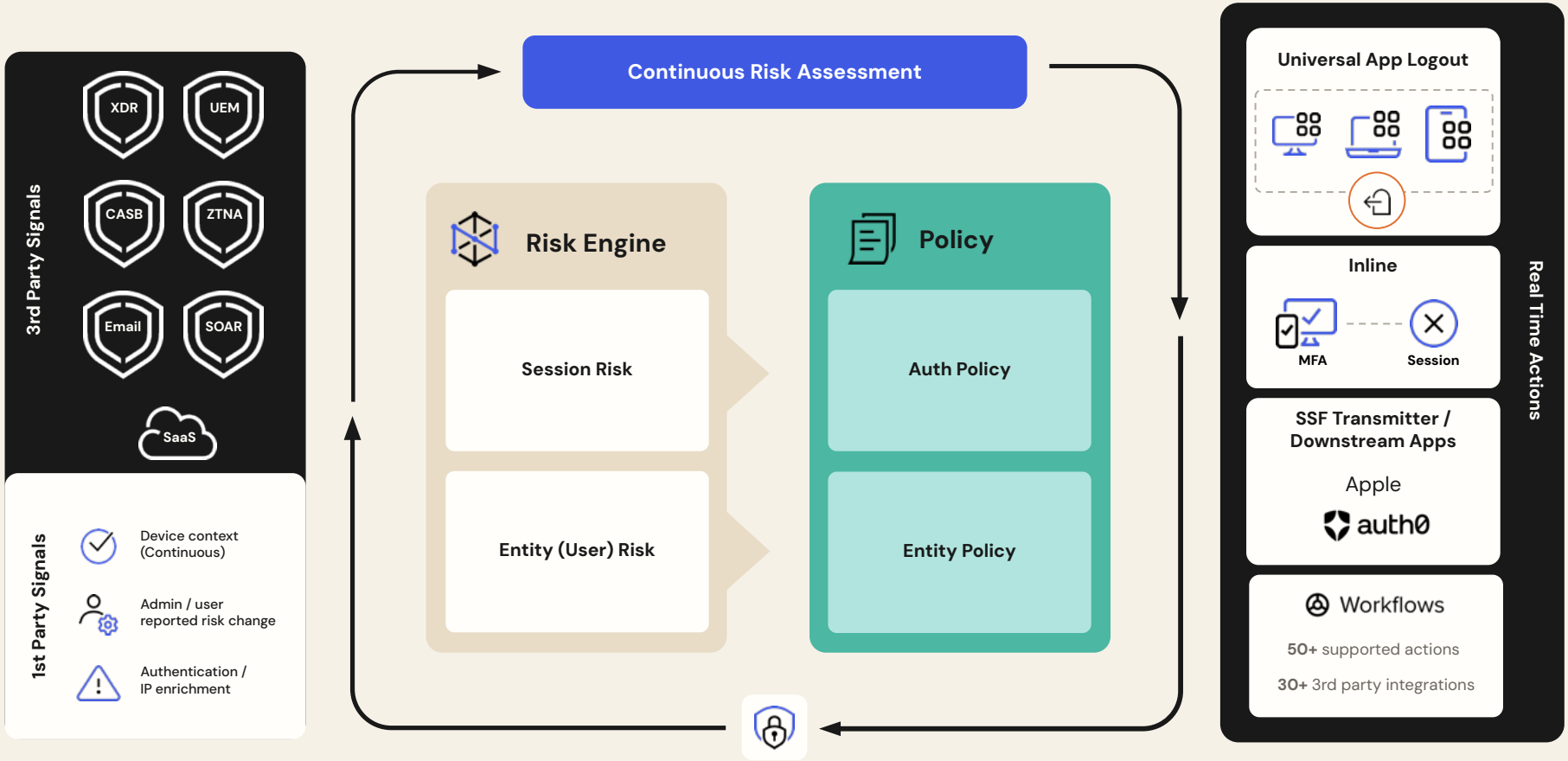


Okta Device Access

Depends on **FastPass** to provide passwordless access post-OS login for a secure passwordless experience from devices to apps

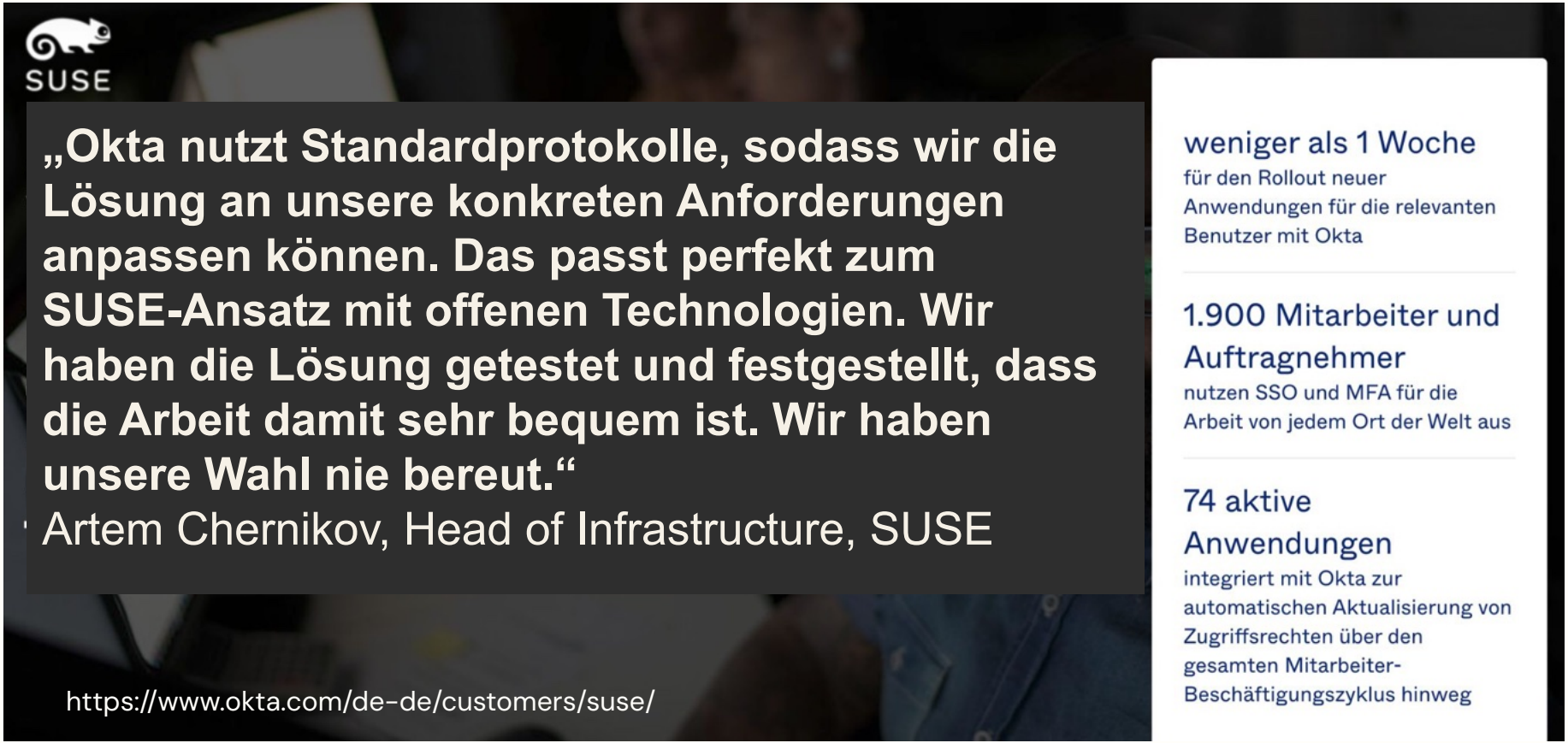


Use risk signals to trigger real-time actions like Universal Logout



okta

Kundenreferenz & Anwendungsfall SUSE



Thank you

okta

The World's Identity Company