Making Zero Trust Possible

Dragan Vladicic

Director, Solutions Engineers APAC, Okta

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; our results of operations may fluctuate more than expected; there may be significant fluctuations in our results of operations and cash flows related to our revenue recognition or otherwise; 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; a network or data security

incident that allows unauthorized access to our network or data or our customers' data could damage our reputation; we could experience interruptions or performance problems associated with our technology, including a service outage; we may not be able to pay off our convertible senior notes when due; 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; and global economic conditions could deteriorate. 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

Business Identity

Personal Identity

Security models are evolving rapidly
Shifting away from the old model of Network as a control plane

61%
of all breaches involve stolen credentials

Verizon DBIR 2021

TRADITIONAL NETWORK

CLOUD-BASED NETWORK

okta

At its foundation, Zero Trust needs to ensure:

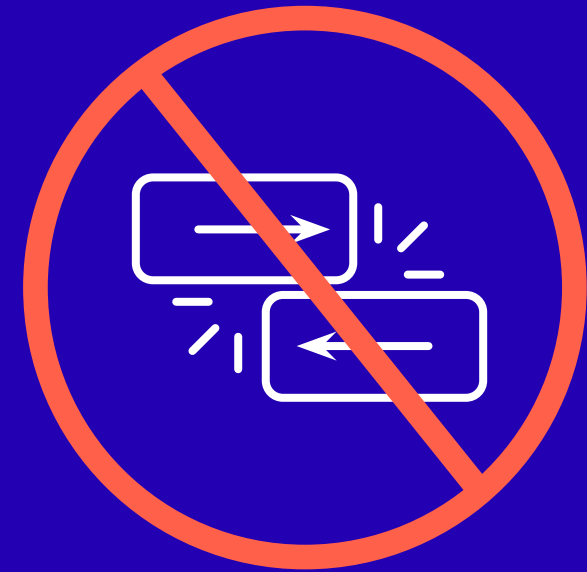The right people

Have the right level of access

To the right resources

In the right context

That is assessed continuously

Least Friction Possible

okta

Zero Trust Maturity Model

Zero Trust is the Ultimate Team Sport

Zero Trust isnt "a" Product

CISA*- 5 Pillars
- Identity
- Devices
- Network / Environment
- Application / Workload
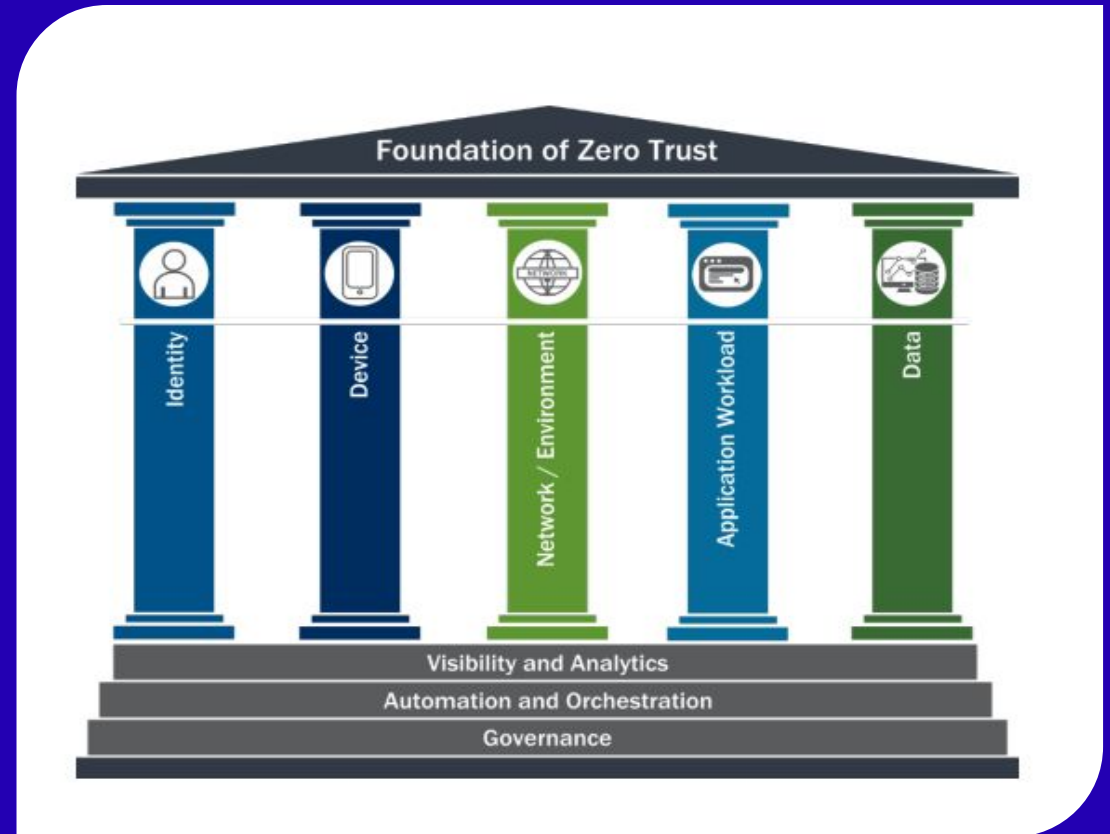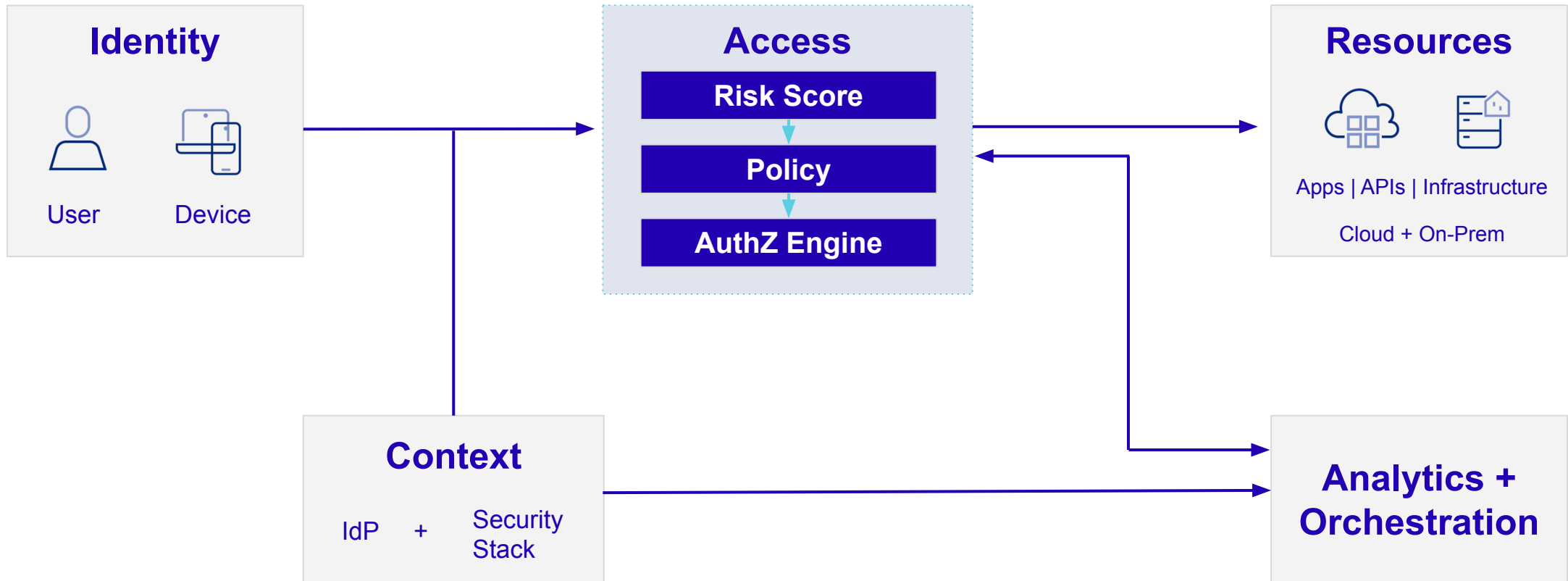- Data

No coincidence Identity is the First Pillar

Figure: Cybersecurity & Infrastructure Security Agency (CISA) Foundation of ZERO Trust*

okta

Modern Identity: Zero Trust Control Plane for All Identities, and All Resources

Identity

User   Device

Access

Risk Score

Policy

AuthZ Engine

Resources

Apps | APIs | Infrastructure

Cloud + On-Prem

Context

IdP   +   Security Stack

Analytics + Orchestration

okta

Integrated with Your Security Stack of Choice
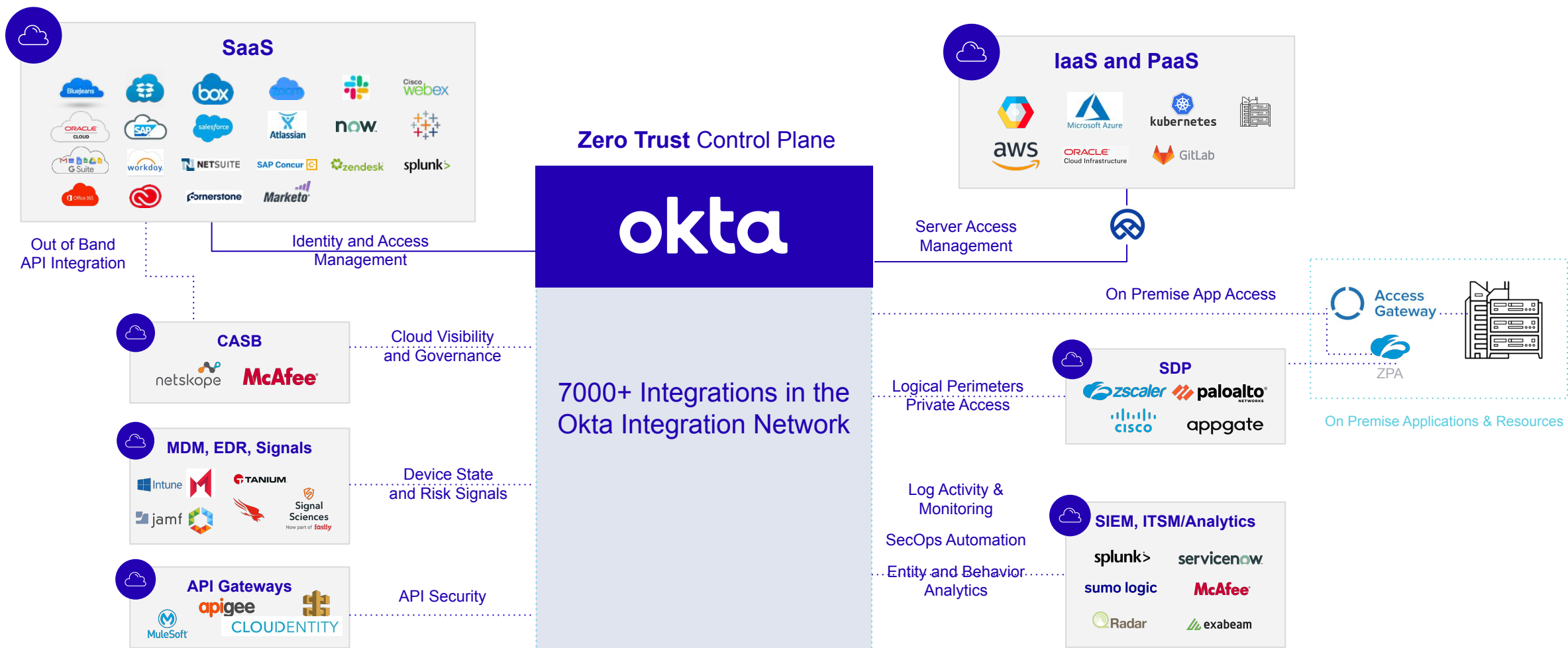
People Perimeter Maturity Curve

Protection

Adoption

STAGE 0

Fragmented identity

- Active Directory on-premises
- No cloud integration
- Passwords everywhere

STAGE 1

Unified IAM

- Single sign-on across employees, contractors, partners
- Modern multi-factor authentication
- Unified policies across apps and servers

STAGE 2

Contextual Access

- Context-based access policies
- Multiple factors deployed across user groups
- Integrated signals from security ecosystem to assess risk posture
- Automated deprovisioning for leavers
- Secure access to APIs

STAGE 3

Adaptive Workforce

- Risk-based access policies
- Continuous and adaptive authentication and authorization
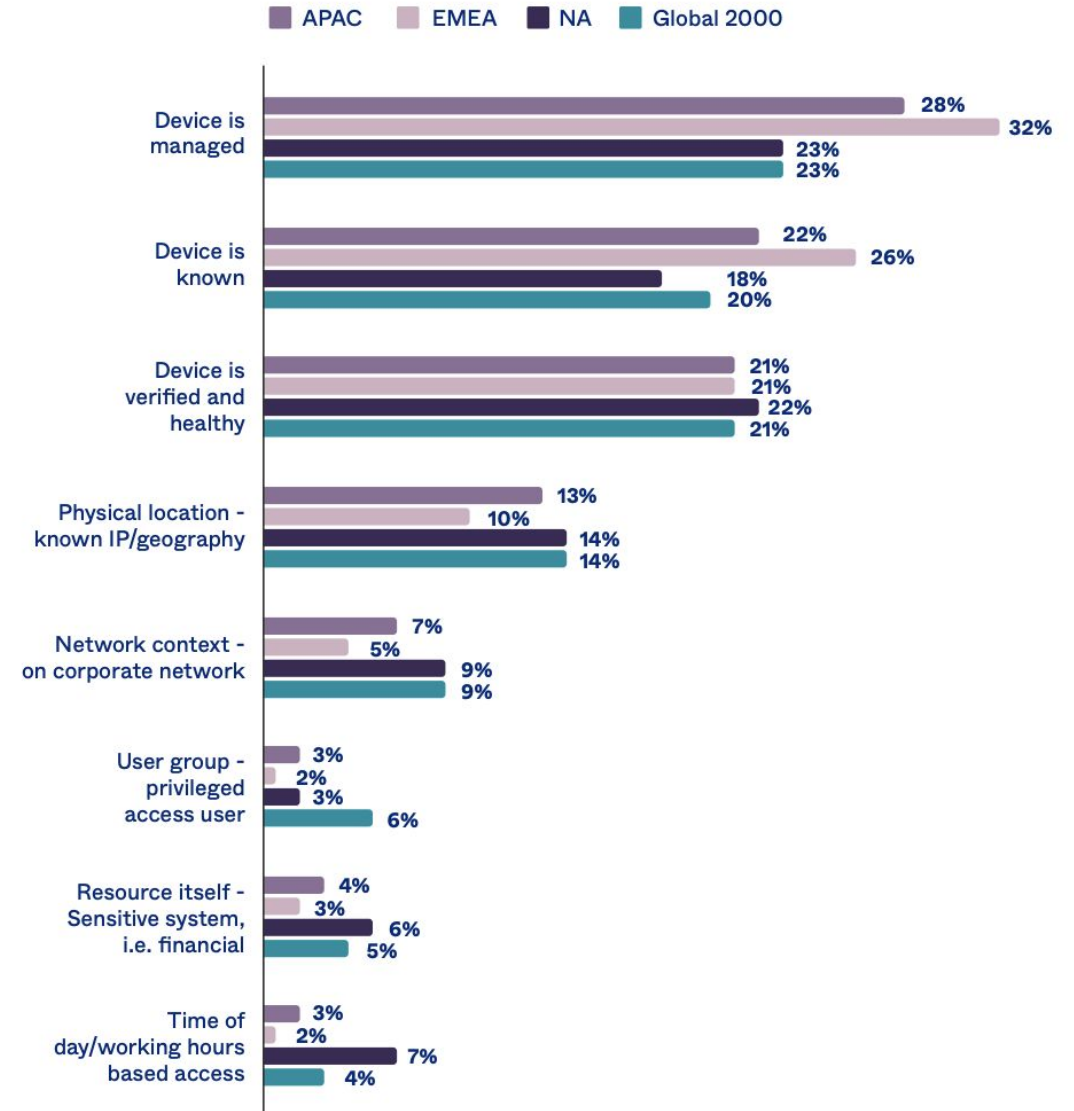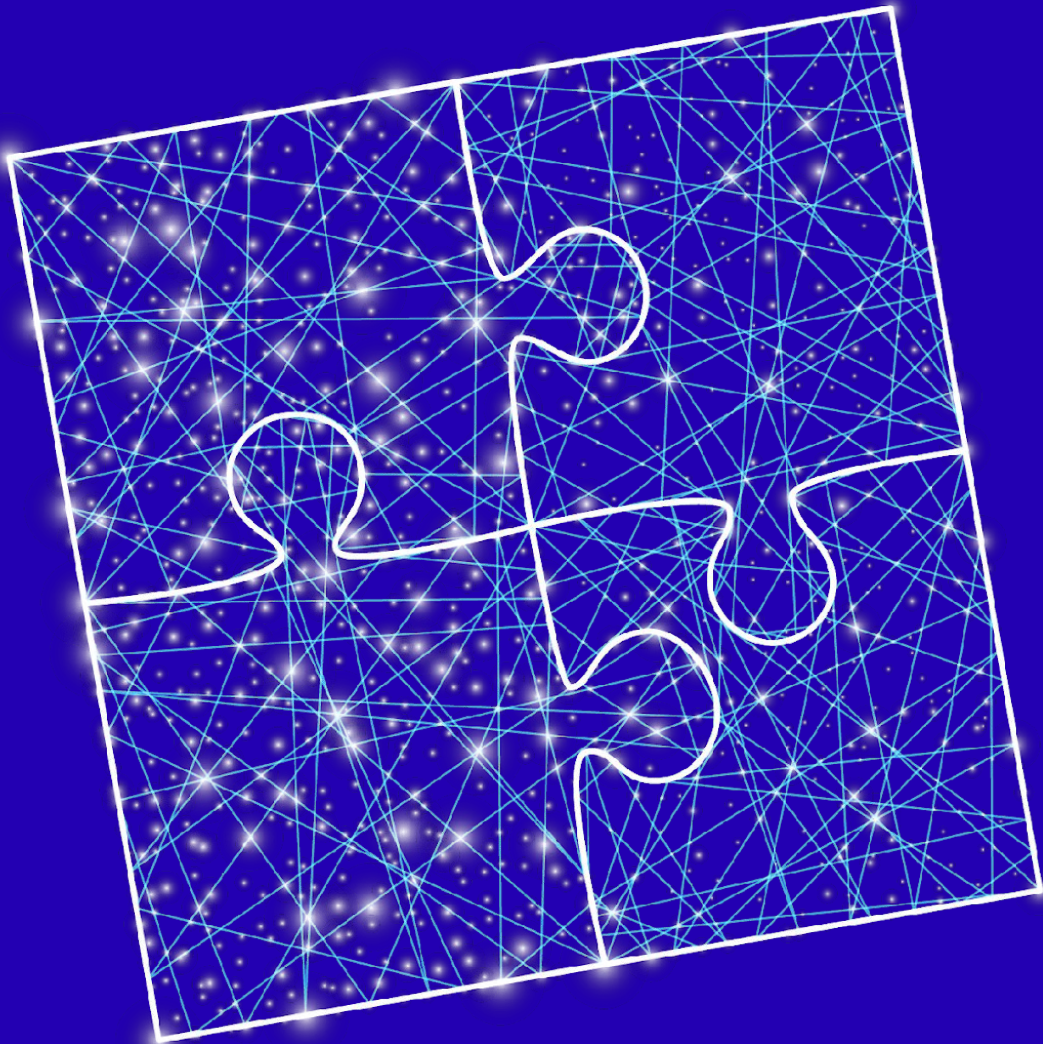- Frictionless access

okta

Device Context is Ranked Highest for Access Decisions

Intune + Okta

- Get the cloud identity and access management benefits like SSO, lifecycle management, and MFA, along with Intune's mobile device management
- Okta's device trust can assess a device's security posture, and use Intune app protection
- Easy transition to a more simple and secure device trust model

What are the top 3 most critical factors you think about when controlling and approving access to your internal resources?

Legend: APAC, EMEA, NA, Global 2000

Factor	APAC	EMEA	NA	Global 2000
Device is managed	28%	32%	23%	23%
Device is known	22%	26%	18%	20%
Device is verified and healthy	21%	21%	22%	21%
Physical location – known IP/geography	13%	10%	14%	14%
Network context – on corporate network	7%	5%	9%	9%
User group – privileged access user	3%	2%	3%	6%
Resource itself – Sensitive system, i.e. financial	4%	3%	6%	5%
Time of day/working hours based access	3%	2%	7%	4%

[7] Okta, "**Businesses at Work Report 2021**," January 28, 2021

A CULTURE OF SECURITY

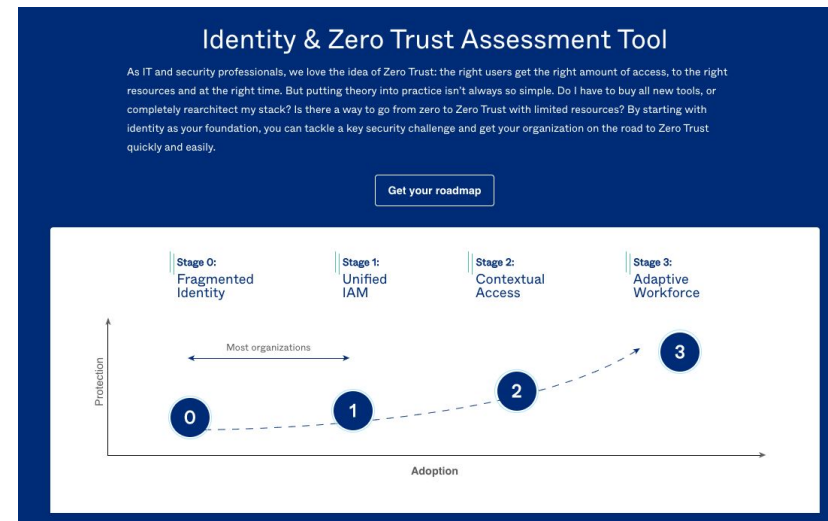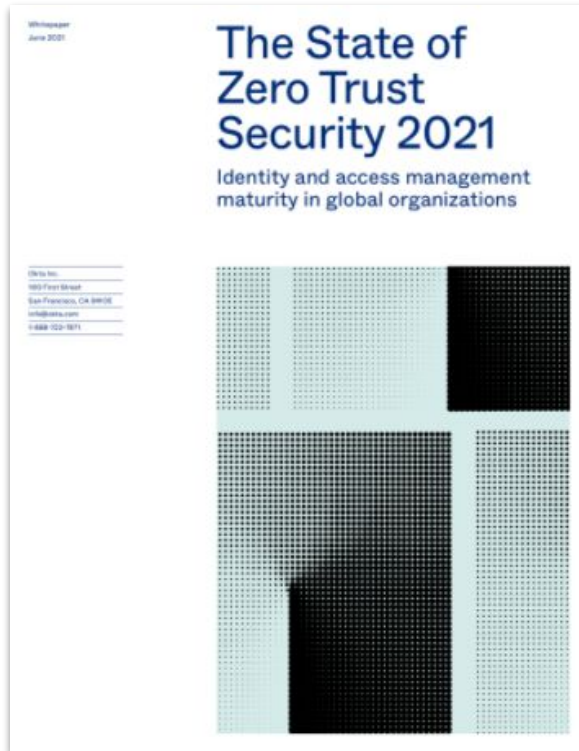There's no silver bullet for Zero Trust

The Zero Trust journey starts with Identity

Okta is a modern Zero Trust Platform

okta

Resources

Okta.com > solutions > adopt a zero trust security model