okta

forum22
EUROPE

Speakers, sessions and key insights

Jump in >

Contents

The future of trust is identity-first

Identity-first customer experience

Identity-first security

Environmental and social governance

Privacy and trust

SESSION 1: THE FUTURE OF TRUST IS IDENTITY-FIRST

Eugenio Pace
CEO, Auth0

The future of trust is identity-first

Trust is critical to building strong relationships between businesses and colleagues, partners and customers. At Okta, we believe it has three components: security, privacy and convenience.

Identity-first security

We're using more apps than ever, at work and in our personal lives, and every connection is an access point for attack. At Okta, 30–50% of the login attempts in our network are bots or hackers – that's billions of malicious logins being stopped per month.

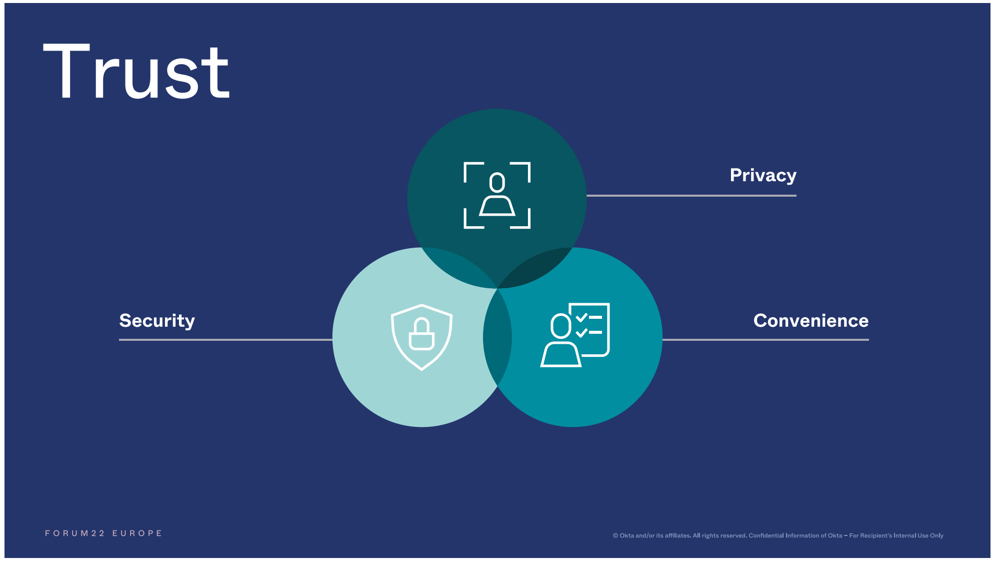
Identity-first privacy

Owners of data expect to have control over what's shared, when it gets shared and how it's revoked, and registration or login is the natural place to start this dialogue. Okta's Digital Trust Survey 2022 showed that users hold service providers responsible for protecting their personal data.

Identity-first experience

People choose convenience over security and privacy. It's why we choose simple passwords like '123456' and reuse them across apps, despite the security risk. But at 60 years old, passwords are nearing retirement, and simple alternatives that are also secure, like MFA, are increasingly popular.

An identity-first strategy can balance and maximise security, privacy and convenience to drive success.



Trust

Privacy

Security

Convenience

FORUM22 EUROPE

© Okta and/or its affiliates. All rights reserved. Confidential Information of Okta – For Recipient's Internal Use Only

80% of breaches in 2021 involved stolen credentials

Watch Eugenio's presentation here

SESSION 1: THE FUTURE OF TRUST IS IDENTITY-FIRST

Yanna Winter, Generali;
Jon Addison, Okta
and **David McClelland**

Fireside chat: Future of identity and trust

How are Okta's customers using identity for their digital transformation journeys?

Jon – The pandemic accelerated digital transformation. Companies pivoted fast to deal with remote working, and systems for managing supply chains and dealing with partners changed overnight. It put traditional organisations with legacy IT under strain. CIOs and chief product officers were in the spotlight and given budget to innovate. Now things are settling down, it's time to see how those new business models stabilise.

How do organisations establish the trust that identity requires, internally and externally?

Yanna – Identity is not an afterthought. That's why we've architected and implemented it from the ground up. We know we'll always work in complex ecosystems, we won't impose the same approach across all of our actors. Okta has been key to working with everything we have, to dealing with all our complexity.

Jon – Establishing trust can be complex, especially with multi-layered ecosystems involving brokers, customers and users. It's challenging to create seamless experiences for all those constituents. We hear a lot of customers talking about identity as a foundational building block – that's what we mean by identity first. It's a foundation for innovation in business.

Read on...

Watch the fireside chat here

Yanna Winter, Generali;
Jon Addison, Okta
and **David McClelland**

Yanna, what's Generali's priority for the next few years?

Yanna – We have 3 key themes – complexity, security & regulatory requirements, and costs. Our employees are a big part of our digital transformation.
One insurance programme can have 200 companies. How do we manage that complexity? Our employees would have to remember thousands of passwords. Without Okta identity management, we wouldn't have a seamless experience for employees.

Jon, what would you like our audience to walk away with today?

Jon – The importance of having an identity-first strategy. Creating experiences that are simple, secure and seamless. Digital transformation should simplify the complex things holding your business back. We need to mirror how consumers use technology, in the workforce. It's about making technology safe, seamless and frictionless to use for everybody.

What does identity-first mean to you?

Yanna – Just before lockdown, I moved house. I didn't have to sign anything physically, or go to anyone's office. Everything was done via a digital identity. It worked beautifully.

Jon – It means putting identity at the heart of your transformation programme. Considering it as a strategic platform. It should be top of mind for everybody.

The pandemic accelerated the pace of digital transformation by 4-7 years

Source: McKinsey

Watch the fireside chat here

SESSION 2: IDENTITY-FIRST CUSTOMER EXPERIENCE

Paul Fisher
Lead Analyst,
Kuppingercole

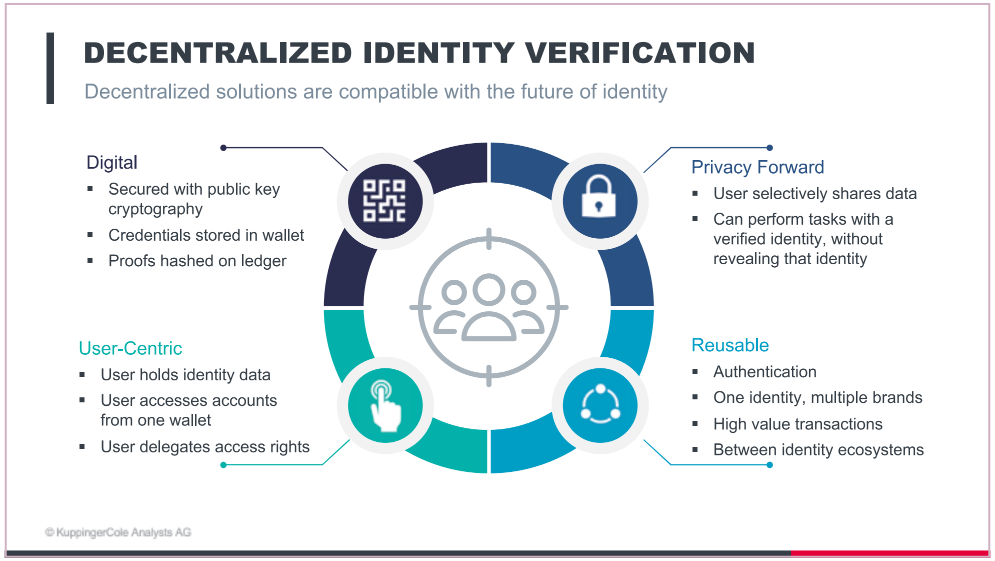
The future of customer experience

Steve Jobs said it best: you've got to start with customer experience and work backwards to the technology, not the other way round. Currently we have a culture where we're focused on security, and we fit customer experience around it – it's something we can improve.

So how do businesses deliver the convenient, private and secure experiences customers today expect? Everyone in the identity industry is grappling with these challenges. We're seeing the emergence of new approaches that could create the seamless authentication experiences of the future. One is digital identity, with users having a digital footprint based on their usage elsewhere online. Another is decentralised identity, or identity component as a service, which takes the best bits from identity platforms and builds something closer to the user.

The identity fabric

This leads to the idea of an identity fabric, a scalable and independent identity 'mesh' around the organisation, rather than a centralised, static identity management platform in the middle of it. Perhaps one day users will choose the organisations they trust with their data – for example, Amazon or a social network – to create a digital identity they can use to verify themselves with any organisation. A truly user-first, technology-second experience that's good for customers, and good for businesses too.



DECENTRALIZED IDENTITY VERIFICATION

Decentralized solutions are compatible with the future of identity

Digital
- Secured with public key cryptography
- Credentials stored in wallet
- Proofs hashed on ledger

Privacy Forward
- User selectively shares data
- Can perform tasks with a verified identity, without revealing that identity

User-Centric
- User holds identity data
- User accesses accounts from one wallet
- User delegates access rights

Reusable
- Authentication
- One identity, multiple brands
- High value transactions
- Between identity ecosystems

© KuppingerCole Analysts AG

> Think about customer experience, first and always, then go to technology

[Watch Paul's presentation here]

SESSION 2: IDENTITY-FIRST CUSTOMER EXPERIENCE

Kalpana Singh
Product Marketing
Leader, Okta

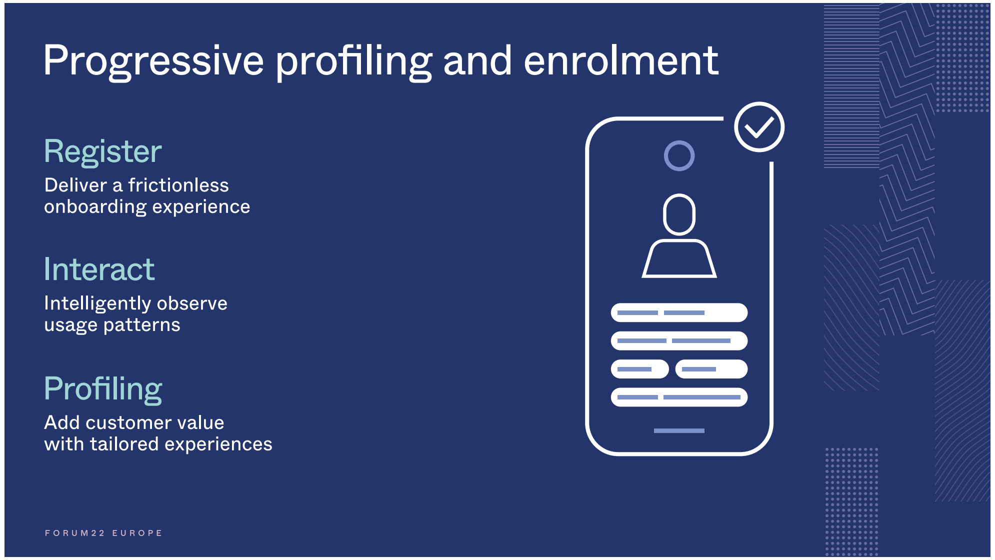
Security vs user experience: a false choice

Every company is now a software company. Companies are in the business of creating apps that bring convenience to consumers, businesses and employees. Our love for seamless Amazon-style experiences is driving our willingness to shop around: 78% would consider banking with a technology firm like Amazon or Google

But convenience falls apart without security. Historically, these two characteristics have been viewed as a trade-off, largely due to inadequate technology and architecture. These days, it's a false choice. We can serve all customers' requirements around security, privacy and convenience with a single, modern identity solution.

Personalisation, at the speed of trust

Such solutions deliver a seamless sign-up experience that allow users to register with minimum information. They then build up a gradual picture of the customer over time, after intelligently observing usage patterns. Perhaps they've noticed a customer check out the credit card section of a banking app, allowing them to follow up with tailored messaging. Or the app can suggest setting up MFA. This is known as progressive profiling and enrolment and it's a powerful tool for deepening customer relationships once brand affinity has been established. Personalisation, at a speed the user is comfortable with.



Progressive profiling and enrolment

Register
Deliver a frictionless onboarding experience

Interact
Intelligently observe usage patterns

Profiling
Add customer value with tailored experiences

FORUM22 EUROPE

77% of online businesses prioritise delivering frictionless user experiences

Source: Sift Digital Trust & Safety 2019

Watch Kalpana's presentation here

SESSION 2: IDENTITY-FIRST CUSTOMER EXPERIENCE

Joop van Heekeren
Enterprise Architect,
CitizenM Hotels

Customer perspective

Since its launch in 2008, CitizenM Hotels has focused on a digital-first customer experience to provide a convenient, consistent service to its customers. A priority was removing some of the small frustrations associated with hotel experience, such as queuing to check in. The company has never had a check in desk at its hotel, instead allowing customers to check in via a self-service kiosk, or since the pandemic, a mobile app.

The company's mobile app is at the heart of CitizenM's customer experience, allowing customers not only to check in and out, but also control room features such as lights, blinds and TV. To encourage customers to download the app, a seamless account creation process is key. Working with Auth0, CitizenM was an early adopter of social login and in 2021 introduced passwordless login via a magic link.

Building deeper relationships

Greater usage of the mobile app also allows CitizenM to build up a deeper customer profile with valuable insights into preferences and usage, such as the temperature they prefer their room to be. As trust builds, customers can choose to do more in the app, such as saving a credit card, allowing for quicker booking direct with the hotel.

Crucially, staff are always on hand to help customers if necessary.
For CitizenM, digital first doesn't need to exclude anyone. Everyone is welcome.

> “Gaining trust is a slow process. If customers' check-in experience is good, they'll download our app.

Watch Joop and David's discussion here

Angela Salmeron
Research Director,
IDC

SESSION 3: IDENTITY-FIRST SECURITY

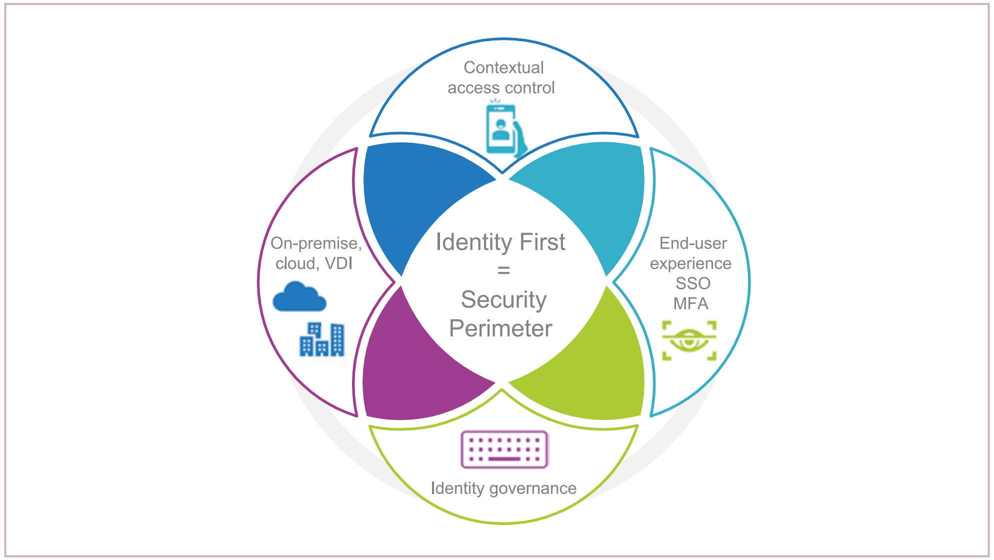
Building a resilient workplace of the future

IDC's research shows the great resignation – or more accurately, the great reshuffle – could see at least 1 in 3 European employees switching jobs soon. After better pay, a better workplace experience is their second highest reason to move (42%). Amid a global talent shortage, building a workplace that will attract and retain the best people is crucial.

Creating an inclusive and equal employee experience regardless of work location is challenging. With remote workers no longer using managed devices and networks, the risk of a data breach is a constant concern for companies, especially those reliant on legacy security systems and tools. And these security breaches aren't due to hackers breaking code – they're stealing credentials. Identity is the new security perimeter.

The borderless organisation

As a result, we're seeing the rise of the borderless organisation, with no premise-based perimeter. At its heart is a Zero Trust architecture that continually verifies and monitors every transaction, allowing businesses to work securely and effectively with remote workers, partners, contractors and customers. Crucial components include SSO, robust identity governance, audit tracking and contextual access and control, which grants access depending on risk and security posture, requiring additional verification factors only when appropriate.


Contextual access control
On-premise, cloud, VDI
Identity First = Security Perimeter
End-user experience SSO MFA
Identity governance

65% Say investing in the digital workspace is a priority

Source: IDC

Watch Angela's presentation here

SESSION 3: IDENTITY-FIRST SECURITY

The shift from tool to strategic – identity's place in the modern security stack

Joe Diamond
VP, Product Strategy,
Okta

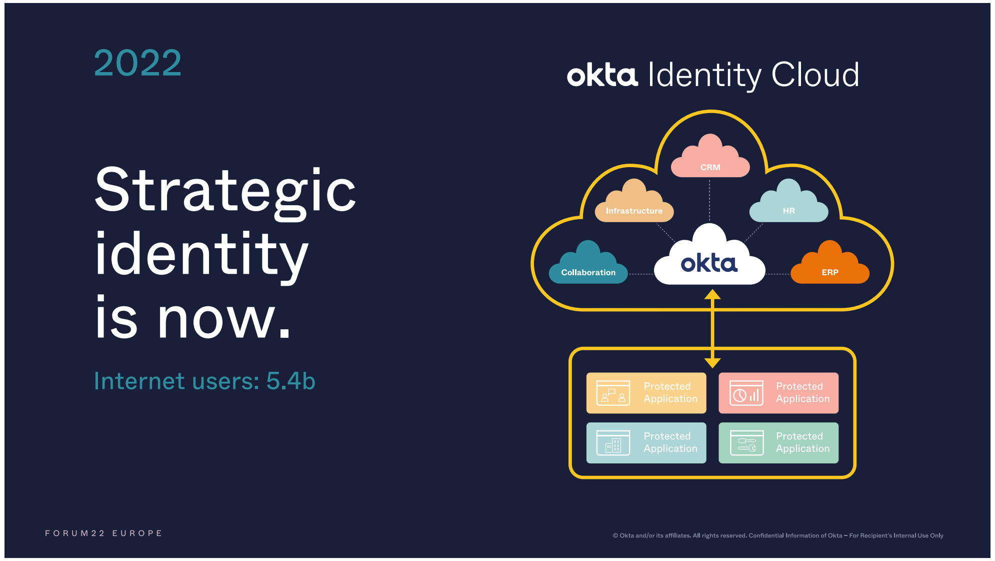
From its somewhat unsexy tactical origins, identity is now the most effective tool in our security stack. Of course, it's always played a monumental role in our history. In the Old Testament, Gileadite soldiers used the password 'Shibboleth' to determine if someone was friend or foe. Mispronunciation resulted in your death, in one of the first incarnations of identity verification.

Cycling through a few centuries, as computer usage exploded in the 20th century, identity was still largely sidelined. Right up until the 1990s, the 'castle and moat' security model centered on networks and devices worked well in an age where workers were still largely shackled to their desks.

A strategic conversation

The 2010s saw the rise of cloud apps, with no way of connecting them to on premises identity architecture. Enter Okta. Identity had become a key control in the IT and security stack. Today, identity is a strategic conversation. It enables the entire security stack. It's independent of device and network. It makes experiences better, from both the consumer and employee perspective. It should hook up to every single application across your stack, and enable every other security control to be effective.

By 2030, 90% of world's population will be online. We need to figure out our approach to identity-first, to enable any app, in any location, on any device, with pervasive security. Let's not Shibboleth this up.



2022

Strategic identity is now.

Internet users: 5.4b

okta Identity Cloud

CRM
Infrastructure
HR
Collaboration
okta
ERP
Protected Application
Protected Application
Protected Application
Protected Application

FORUM22 EUROPE

© Okta and/or its affiliates. All rights reserved. Confidential Information of Okta – For Recipient's Internal Use Only

> Today, identity is a strategic conversation. It enables the entire security stack.

Watch Joe's presentation here

SESSION 3: IDENTITY-FIRST SECURITY

Mads Grandt
Global ICT Specialist Adviser,
Norwegian Refugee Council

Customer perspective

Established 75 years ago, the Norwegian Refugee Council helps people around the world forced to flee armed conflict and violence. The organisation is complex in the people, places and interfaces it serves, with 16,000 aid workers and operations in 35 countries, many of which are hard-to-reach locations due to their geography or ongoing conflict.

In such an expansive and remote network, identity and trust are important. When staff are connecting, the organisation needs to be sure people are who they are, to protect their systems from misuse. The notion of an inside or outside network is redundant. The business uses Okta to challenge and verify every login attempt, choosing an appropriate MFA method depending on what tokens may be available in the user's location.

Supporting a diverse workforce

Since implementing Okta in 2016, the NRC now has almost 100 apps connected via Okta, utilising solutions such as SSO for rapid deployment, Lifecycle Management for automated account deactivation, and MFA for additional security with minimal friction. Okta has been crucial to its technological transformation, enabling it to adopt new apps at scale, support the huge growth in its workforce and accommodate the varying degree of digital literacy among its diverse workforce.

Watch David and Mads' discussion here

SESSION 4: ENVIRONMENTAL AND SOCIAL GOVERNANCE

Charlotte Challis
Principal Carbon Consultant,
Anthesis Group

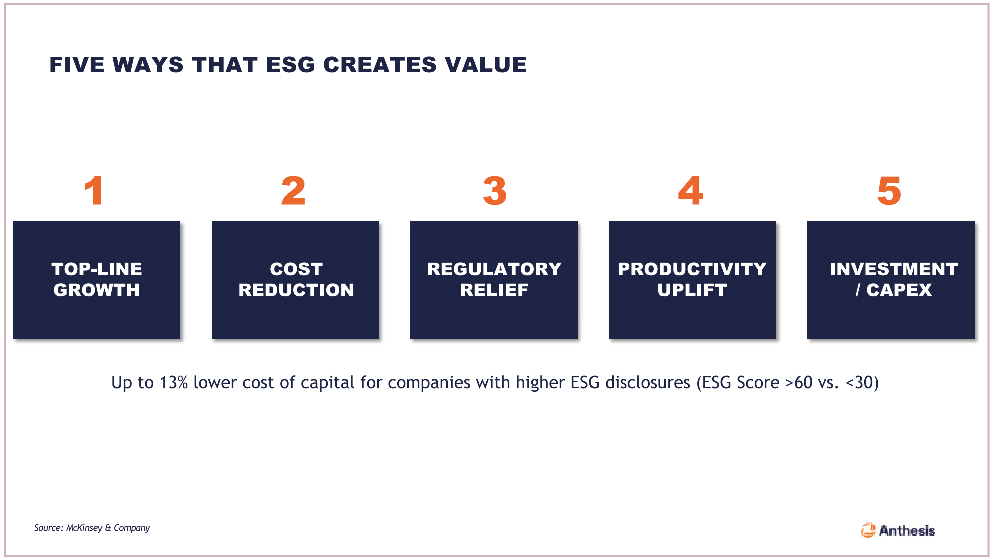
Why ESG is a business imperative

Environment, Social, and Governance (ESG) has moved from niche to mainstream in the last few years, with the recognition that we're in a decisive decade for our climate. Building ESG into the heart of the business builds trust, from which we can create new products, access new markets, and reach new customers. But having ESG at the heart of the business also brings opportunities: McKinsey found that 70% of consumers said they would pay an additional 5% for a green product with the same performance.

ESG at the heart of business

To have real benefits, ESG cannot be just box ticking. Setting science-based targets that reduce emissions in line with the levels necessary to keep global warming to 1.5 degrees, is vital. One way in which businesses are embedding ESG principles into how they operate is to use Internal Carbon Pricing, which quantifies the cost of carbon to the business in $ per ton of CO_2. This can be used to evaluate the carbon impact of procurement decisions, for example.

Internal carbon pricing is just one example of how organisations can embed ESG and prepare for a carbon constrained future. Those that are making these changes are aligning value creation with tangible positive impact.



FIVE WAYS THAT ESG CREATES VALUE

1 TOP-LINE GROWTH

2 COST REDUCTION

3 REGULATORY RELIEF

4 PRODUCTIVITY UPLIFT

5 INVESTMENT / CAPEX

Up to 13% lower cost of capital for companies with higher ESG disclosures (ESG Score >60 vs. <30)

Source: McKinsey & Company

Anthesis

70% of consumers would pay an additional 5% for a green product

Source: IDC

Watch Charlotte's presentation here

SESSION 4: ENVIRONMENTAL AND SOCIAL GOVERNANCE

Alison Colwell
Director Environmental,
Social and Governance and
Sustainability, Okta

Embracing ESG goals through hybrid working

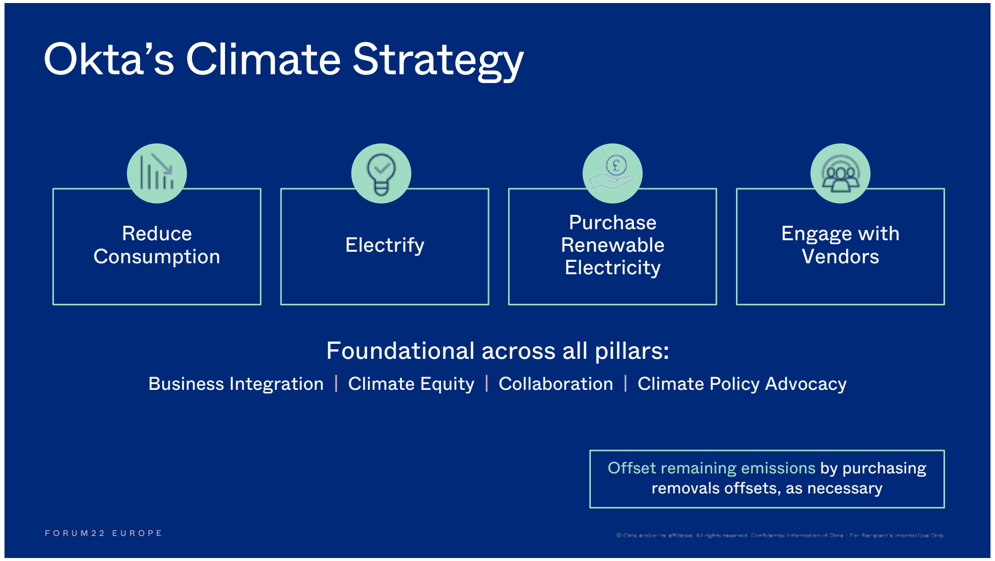
At Okta, we're integrating climate into our key decisions and operations, with 4 key aims: reducing consumption, switching from natural gas to electricity, purchasing renewable electricity, and working with our vendors to reduce the emissions in our value chain.

Trust starts with transparency: a core Okta value. We're increasing the amount of information we share with partners, employees, investors on our environmental performance. We submitted our climate performance to the Carbon Disclosure Project for the first time last year and we're working on improving our B minus rating.

Like other businesses, we're experiencing a huge shift in the way we work. We now cover our remote workforce electricity consumption with 100% renewable electricity. To do this, we're purchasing renewable energy certificates from schools and community-based organisations that seek to make renewable energy more accessible and affordable.

Supporting our customers

As vendor to our customers, we also want to support them in achieving their emission reduction targets. Today we've achieved 100% renewable electricity for Okta's cloud service providers – exciting, because as we grow, we can continue to offer our customers a more sustainable platform.



Okta's Climate Strategy

Reduce Consumption

Electrify

Purchase Renewable Electricity

Engage with Vendors

Foundational across all pillars:

Business Integration | Climate Equity | Collaboration | Climate Policy Advocacy

Offset remaining emissions by purchasing removals offsets, as necessary

FORUM22 EUROPE

> Today we've achieved 100% renewable electricity for Okta's cloud service providers

Watch Alison's presentation here

SESSION 5: PRIVACY AND TRUST

Bianca Lopes
Identity Advocate for Humanity,
Sustainability and DeFi investor

The future of privacy

We live in a world where we've curated versions of who we truly are. In a world and society where we've traded emotions for push notifications, friends for followers, value has a new meaning and category. Data is the largest asset class we're building. We put just about everything online, but in doing so we've created a messy situation. How do we fix our problem with identity?

Let's start with where it came from. Most enterprises and identity journeys started with a simple physical presence and channels to serve users. Most identity systems involve siloes. We've been protecting information by building walls – often one on top of the other.

Redefining identity

We need to redefine identity through the lens of permission and access. Fundamentally, the number of versions of you are growing – and growing in channels that enterprises no longer control. Identity is now a data game – an attribute conversation.

Let's stop having conversations about IAMs and siloes, and start understanding the power of a proper identity that is founded on attributes, with the clear understanding that no one owns anything. Web 3 and decentralised finance will force us to rethink identity strategy, and in doing so, rebuild trust with customers.

> Identity is now a data game – an attribute conversation.

Watch Bianca's presentation here

SESSION 5: PRIVACY AND TRUST

Ben King
VP, Customer Trust,
Okta

Navigating trust through the LAPSUS$ incident

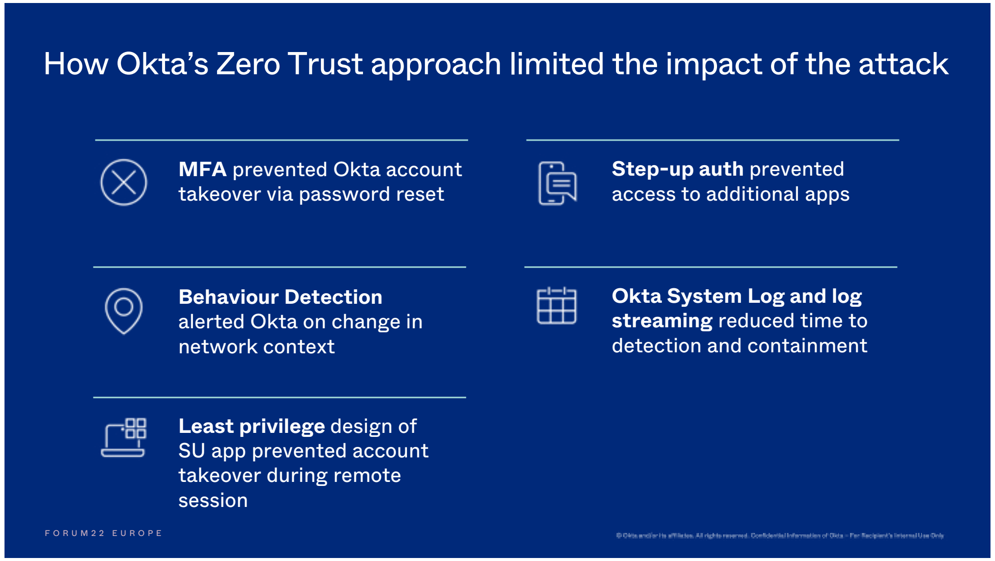
In January 2022, Okta detected an attempt to compromise the account of a third-party customer support engineer working for one of our sub-processors. Their security team engaged a third-party forensic security team who, in their report, assured Okta there had been no scope for compromise of Okta or our customers.

Days after this report, LAPSUS$ – a well-known threat actor who had also targeted Microsoft and LG in previous weeks – released their screenshots. There was much speculation among the media, but at Okta we needed to run our own investigation to determine what had really happened.

By April, the full picture emerged. The malicious activity took place on one day, 21 January, and lasted for 25 minutes. Two customers were affected. Due to the least privileged design of the support tool, the impact of the data viewed was low risk. Okta's Zero Trust approach to access had limited the options the actor had to gain access to systems or do any damage beyond screenshots. MFA, behavioral detection, least privileged design, and log streaming all did their job in enabling the incident to be contained and run into the ground quickly.

Lessons learned

We know we could have done better in how we responded to this event and its communication, and we're determined to learn lessons. We're improving how we govern third party risk, by mandating that suppliers with access to customer data use Okta identity and Okta managed devices. We're launching a customer support tool, to give customers more control over the data a support engineer can see. And we're making it faster and easier for Okta to share data with our customers' security teams.



How Okta's Zero Trust approach limited the impact of the attack

MFA prevented Okta account takeover via password reset

Step-up auth prevented access to additional apps

Behaviour Detection alerted Okta on change in network context

Okta System Log and log streaming reduced time to detection and containment

Least privilege design of SU app prevented account takeover during remote session

FORUM22 EUROPE

> The Zero Trust security framework worked as well in this real world scenario, as it had promised in theory

Catch up on Forum22

SESSION 5: PRIVACY AND TRUST

Enza Iannopollo,
Bianca Lopes, Ben King
and **David McClelland**

Panel discussion – building trust through privacy

What are the first steps to achieving privacy and trust?

Enza – There are two basic steps. The first is to understand which requirements apply to you – there are 137 countries with different privacy regulations and businesses must define the key common principles they should focus on. The second is to think about data. In the past, data was a defined bucket. Today, personal data is every attribute that can directly or indirectly relate to an individual identity. It's the duty of organisations to understand the relationship between attributes, and protect it.

What challenges and pitfalls do organisations face?

Ben – The international landscape is significant. It's one thing to build an app with privacy in mind for a particular geography, but if your app scales internationally, that's a challenge. There's also the 'scariness factor' – the interplay between privacy and innovation. When I worked in a bank, we could anticipate what customers' next purchases would be based on their spending habits, and ask very specific questions. But we had negative feedback – people felt it invaded their privacy.

Read on...

Catch up on Forum22

Enza Iannopollo,
Bianca Lopes, Ben King
and **David McClelland**

What are the next steps as we move to a decentralised model of identity?

Bianca – Businesses must redefine their current practice of identity. When you look at the construct under which you build AML and KYC practices, you get to a data-level understanding of the power of every single piece of what you know. The process of providing value as a company is going to look different – it's going to look decentralised from a data perspective, because you can't do everything alone. Technologies are changing too fast. It's about letting go of control.

Enza – You need to know your ecosystem too. As a business sharing data with other businesses, it's difficult to keep control. You can use technology to understand what's happening, but governance and processes and due diligence still have to apply. It's important to understand who are your partners, what they're doing with your data, and what boundaries you can put in place to protect it.

What's coming next for identity?

Ben – We can put the ownership of identity to the individual citizen, but they're probably not the best people to secure it for themselves. The controls we build around the outside, while giving the power to people, are important – to own their identity, and go forth and do amazing things.

Catch up on Forum22

okta

forum22
EUROPE