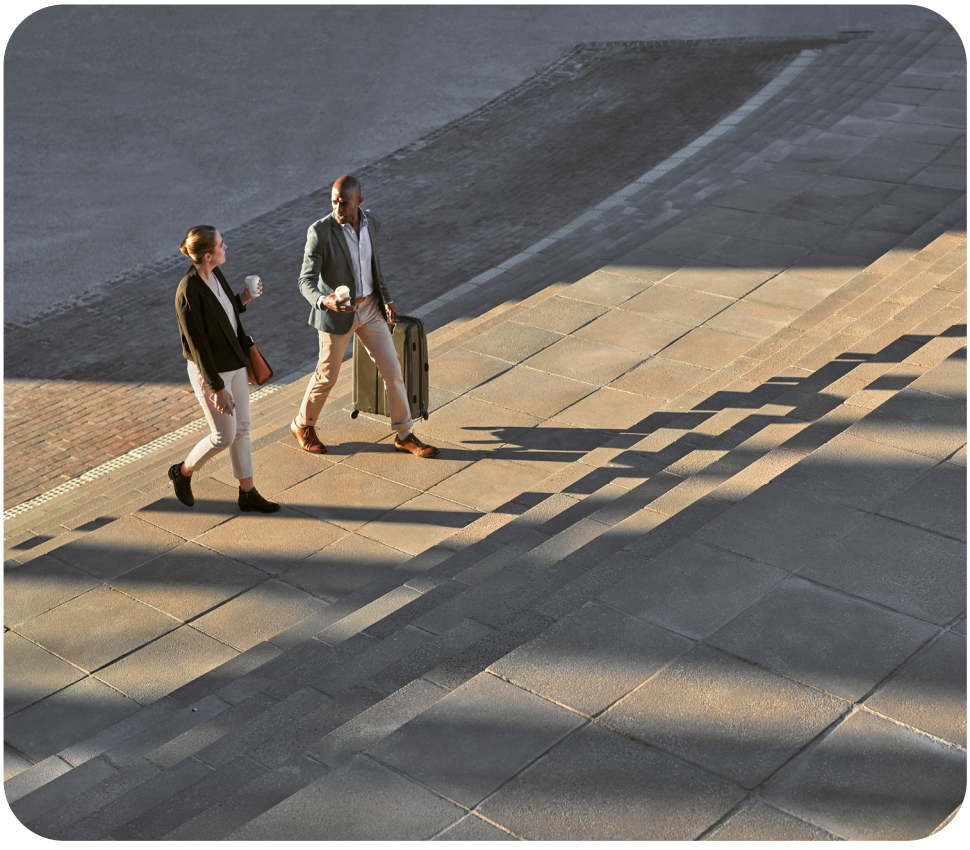
Guide

Can you balance IT security, resilience & accessibility in the public sector?

Okta Identity Insights

okta

Contents



Introduction

All too often, IT teams in UK councils find themselves compromising security and resilience at the hands of accessibility. And while this shift in balance may have been necessary to ensure operations could continue during the pandemic, rapidly rising cybercrime and the switch to hybrid working has forced IT leaders to reassess their strategies.

While providing citizens and employees with seamless access to all the apps and platforms they need remains a key priority, UK councils must also ensure all their data is kept private and secure. But what challenges will they encounter when balancing the scale between security, resilience & accessibility, and how can an Identity-first approach help?

In this guide, we use insights from the recent Okta Public Sector podcast with Tech Journalist David McClelland and Kevin Butler, Principal Solutions Engineer at Okta, to discuss how a cloud Identity solution can help create the modern, digital-first government IT systems fit for today and tomorrow.

David McClelland

Kevin Butler

Watch the podcast

Challenge 1: accessibility

Embracing technical innovation

Like many organisations today, UK councils are undergoing huge transformations to modernise their on-premises services and applications. While keeping the lights on was a key focus during the 2020 lockdown, the priority pushing forward is to embrace the technological innovations that satisfy growing demands for safer and more convenient digital experiences.

However, updating these services and apps while trying to keep them as secure as possible will often incur huge costs, drain time, and require an abundance of resources that many local councils simply don't have. The result leads to a breakdown in operational performance, frustrated citizens and employees, and an increase in security gaps for bad actors to exploit.

Long-term support for hybrid working

Over the past two years, remote and hybrid working have become an integral part of our daily lives. While initially a short-term response to the pandemic, research shows that 42% of employees today expect a mix of both home and office-based working[1], and councils must comply.

Yet, managing this rapid shift in working practices has proved a major challenge for IT and Security teams in the public sector. As well lacking visibility and control over which users can access what resources, providing consistent, secure access to on-premises infrastructure remotely is far from simple.

[1] The New Workplace Report

Challenge 2: security

Rising ransomware and credential-based attacks

As ransomware and credential-based cyberattacks continue to soar, IT and security leaders face immense pressures to protect their citizens and workforce from harm. Alongside the crippling financial impact, a security breach can also cause irreparable damage to local council's reputation as a trustworthy service provider.

While patching systems and educating employees on the dangers of cybercrime is essential, these procedures take time to complete and do little to protect IT networks in the present day. Instead, a more intense focus on digital identities and their role in helping IT and Security leaders easily identify which users have access to what resources is critical.

Implementing Zero Trust without disrupting operations

In the hybrid workplace where traditional castle-and-moat security models no longer apply, adopting a Zero Trust approach that assumes risk in everyone and everything unless proven otherwise by Identity is the only way to keep networks secure.

Yet, locking down access without bringing workflows to a grinding halt remains a key challenge for IT and Security leaders in the public sector. Though cyberattacks remain a critical focus point, this drop in productivity can be equally (if not more so) damaging to operational performance and the level of care citizens receive.

Challenge 3: resilience

Providing failsafe digital services

Citizens and employees today are more demanding than ever before. They want round the clock access to all the apps and resources they need to work or communicate with their government – and they expect councils to satisfy their needs.

Maintaining these applications and keeping them running 24/7, however, places huge strain on IT and Security staff. As well as increasing the risk of security breaches through human error and a higher turnover of staff, the need for surplus hardware investments cuts even further into IT budgets that are already over stretched.

How can an Identity-first approach simplify this journey?

Simplify the user login process with Single Sign-on

Usernames and passwords are the bane of any login experience. As well as being difficult to remember and easy to forget, they're often the primary target for bad actors to attack. To simplify the login process and give citizens, employees, partners and suppliers fast, secure access to the apps and platforms they need, many UK councils now turn to technologies like Single Sign-on for a solution.

Citizen benefits.

- Delivers secure and convenient passwordless access
- Enables one single Identity across the entire council
- Eliminates the need to re-register for 10 or 15 services i.e., the bins, the car parking, the council tax, or the rent

Employee benefits.

- Provides seamless access to all the apps they need to work
- Removes the need for multiple passwords for multiple apps
- Increases productivity and lets employees focus on priority tasks

IT & Security benefits.

- Consolidates user access controls across all IT systems
- Simplifies user access auditing and helps maintain compliance standards
- Integrates with 7,500+ apps to accelerate deployment

Strengthen security with Multi-Factor Authentication

If Single Sign-on is the key for smoother login experiences, then Multi-Factor Authentication (MFA) is what ensures every login attempt is safe and secure. By adding an additional layer of authentication whenever a user signs into an application or platform, MFA significantly reduces the risk of credential-based attacks without impacting the user experience.

Citizen benefits.

- Securely authenticates with minimal friction
- Eliminates the need for traditional usernames and passwords
- Verifies identities from whichever device is most convenient

Employee benefits.

- Protects sensitive data without compromising productivity
- Enables secure working from any device or location
- Recognises previously authenticated devices to reduce authentication prompts

IT & Security benefits.

- Automatically challenges or blocks logins from suspicious devices
- Significantly reduces the risk of credential-based cyber attacks
- Meets all data privacy and compliance standards

Automate provisioning and deprovisioning with Lifecycle Management
Considering the huge volume of user accounts that UK councils must manage daily, provisioning apps and services manually can be incredibly challenging. As well as draining precious time and resources, failure to supply citizens, employees, partners, and suppliers, with the apps they need as soon as they need them can breakdown workflows and irreparably damage user experiences across the board.

By automating key provisioning and deprovisioning processes with a modern identity solution like Okta, UK councils can reap the following benefits.

Citizen benefits.

- Gives every employee instant access to the apps they need from day one
- Automatically upgrades access rights as employee moves to new roles
- Accelerates offboarding while ensuring employee can still access benefits such as pensions, payslips etc. after they've left the organisation

IT & Security benefits.

- Frees up resources by automating onboarding/offboarding processes
- Automatically switches off access for suspicious user accounts
- Maintains full compliance and ensures rules are applied correctly

Increase resilience with cloud-first Identity

In a fast-moving digital-first world, Identity is the glue that holds everything and everyone together. Security, operational performance, and citizen trust all rely on having a strong, resilient Identity and Access Management platform in place.

While building, managing, and maintaining these complex technologies in house can place huge strain on UK local council IT and Security teams, outsourcing the task to a trusted cloud-first identity provider provides the following benefits.

Citizen benefits.

Enables round the clock access to all digital council services

- Is instantly available across all laptop and mobile devices
- Provides high level security with minimal friction

Employee benefits.

- Instantly integrates with all business-critical cloud and on-prem apps
- Adequately supports remote and hybrid working
- Requires no manual installations on end user hardware

IT & Security benefits.

- Managed on a 24/7 basis by service provider
- Reduces identity and access management downtime by 99.99%[2]
- Eliminates hardware costs – both investment in new tech and maintenance of existing systems

[2] Okta Raises the Industry Bar With 99.99% Uptime for Every Customer

Accelerate Zero Trust Maturity

While there's no silver bullet when it comes to achieving a Zero Trust security architecture, the journey is much faster when identity sits at its core. By investing in a modern Identity and access management platform like Okta, UK councils can quickly eliminate many of the most common cybersecurity threats while providing seamless access to users located outside traditional IT network perimeters.

Employee benefits.

- Ensures the right people have the right level of access to the right resources
- Provides strong security without adding friction to the user
- Eliminates the risk of credential-based attacks

IT & Security benefits.

- Instantly deployable across the entire IT ecosystem
- Consistently verifies identities without adding friction for the user
- Unifies access across all IT systems – both on-premises and in the cloud

Why should UK councils trust in Okta?

Improves total cost of ownership
With Okta, our customers can benefit from market-leading cloud identity from day one. We provide future-proof protection across all IT systems, and we build, manage and maintain the technology on your behalf using our team of dedicated Identity specialists.

Simplifies the complexity of Identity management
While managing Identity and Access Management in-house can be challenging, outsourcing to a trusted provider like Okta allows you to reap all the benefits with none of the pain. We remove the complexity of on-site hardware installations and management, and we support your organisation as it moves into the cloud – allowing you to retire on-site apps and platforms gradually at whatever pace is most comfortable.

Eliminates friction while maintaining security standards
Out elite suite of world-leading Identity products are simple to use and can be deployed quickly across your entire network within days. While highly effective at mitigating many of the most common forms of cyberattacks, they provide little friction for the end user and ensure all security and data privacy standards are met consistently.

Reduces legacy debt
As an agile cloud-first Identity platform, Okta provides instant innovation over the top of any IT system and requires no further investments in on-premises technology. We also offer more than 7,000 ready-built integrations with many of the most common cloud and on-premises apps, ensuring you get a full return on both new and existing technology investments.

For more information on how Okta can help balance IT security, resilience & accessibility in your council, please click for more information or schedule a call with one of our friendly experts today.

Learn more | Book a call

okta

EMEA Headquarters
20 Farringdon Road
London EC1M 3HE, UK
info_emea@okta.com
+44 203 389 8779