ZERO TRUST FOR
LOCAL GOVERNMENT

Securing England's Biggest Council Shake-Up in 50 Years

How ZTNA and SSE enable cost-efficient, low-risk transition for councils navigating Local Government Reorganisation



©2026 Zscaler, Inc. All rights reserved.

WHITEPAPER

Executive Summary

England is undergoing the most significant restructuring of local government in over 50 years. The Government's Local Government Reorganisation (LGR) programme will abolish hundreds of county and district councils, replacing them with new single-tier unitary authorities by vesting day, 1 April 2028 for most areas. In Essex alone, 15 councils are being consolidated into five. Across 21 two-tier areas, over 70 reorganisation proposals are under consideration.

For technology and digital leaders, this is not an administrative exercise. LGR is the equivalent of a major corporate merger, but with an immoveable legal deadline, no option to walk away, and the full weight of public scrutiny on every operational failure.

This paper argues that Zero Trust Network Access (ZTNA) and Secure Service Edge (SSE), alongside associated capabilities in Data Loss Prevention (DLP), AI security governance, and employee experience monitoring, represent the most practical, cost-effective, and risk-reducing approach to managing the IT and security challenges created by LGR. These are not technology solutions in search of a problem: they directly address the specific, time-pressured, multi-organisation challenges that every council undergoing reorganisation will face.

©2026 Zscaler, Inc. All rights reserved.

THE CORE ARGUMENT IN THREE SENTENCES:

- **LGR creates a predictable surge of access,** data, and security risk across multiple predecessor organisations operating simultaneously under a new governance structure
- **Traditional network-centric approaches** (VPNs, firewall rules, IP address management) cannot scale fast enough, cheaply enough, or safely enough to meet vesting day
- **ZTNA and SSE decouple secure access from the underlying network,** enabling councils to give the right people access to the right systems from day one, regardless of which legacy environment they sit in

1. The LGR Challenge: What Is Actually Happening

1.1 Scale and Timeline

In December 2024, the Government published its English Devolution White Paper, announcing the end of two-tier local government in England. The programme requires county and district councils, which share responsibilities between an upper and lower tier, to be replaced by single-tier unitary authorities serving populations typically above 500,000 residents.

The timetable is aggressive. Surrey's new unitaries (East Surrey and West Surrey) held their first elections in May 2026 and go live on 1 April 2027. For the majority of the 21 invited areas, elections are expected in May 2027 with vesting day on 1 April 2028. Shadow authorities, bodies elected but not yet legally empowered, will operate from mid-2027 onward, creating an extended period of dual-running and organisational uncertainty.

1.2 The Three Types of Structural Change

Not all councils face the same LGR scenario. There are three principal patterns, each with distinct operational implications:

- **Merger. Merger:** Two or more existing councils (typically districts within a county) merge to form a new unitary. Staff, systems, and data from both organisations must be brought together.
- **Dissolution.** Dissolution and transfer: A council, typically a district, is abolished and its services, staff, and data are absorbed by a new or existing unitary. The dissolved council's network and IT estate must be wound down in a controlled manner.
- **Boundary change.** Boundary adjustment: A council loses or gains parishes, wards, or territories. Smaller in scope, but still requires access to systems that may sit in another organisation's environment.

Many councils will face combinations of all three. Essex's consolidation from 15 to 5 authorities involves elements of every pattern simultaneously.

©2026 Zscaler, Inc. All rights reserved.

1.3 The M&A Parallel

LGR is structurally analogous to corporate mergers and acquisitions. The same challenges arise: how do you give employees from Organisation A access to the systems of Organisation B on day one? How do you prevent data from flowing to the wrong place during transition? How do you maintain operational continuity while unwinding a legacy IT estate?

The critical difference from corporate M&A is that councils cannot defer the deadline, negotiate an extension, or accept a service degradation. Statutory services (social care, housing, planning, waste, benefits) must continue uninterrupted. The political and reputational consequences of a failed vesting day are severe and immediate.

2. The Technology Problem LGR Creates

2.1 Inherited IT Complexity

Councils undergoing LGR will inherit multiple discrete IT estates. Each predecessor organisation will typically have its own:

- **Network architecture:** separate MPLS circuits, SD-WAN configurations, or hub-and-spoke topologies built around specific data centres and office locations
- **VPN infrastructure:** different vendors, different client software, different authentication mechanisms
- **Firewall estates:** different rule sets, different IP addressing schemes, potentially overlapping address ranges that create routing conflicts
- **Identity and directory services:** separate Active Directory forests or Azure AD tenants with different user naming conventions, group structures, and access policies
- **Security tooling:** different endpoint protection, SIEM platforms, and monitoring capabilities — or no monitoring capability at all

The Local Government Association has identified that the scale of merging or separating systems and data securely 'can feel overwhelming', and that cyber security is frequently under-resourced in early LGR planning despite being critical to transition success.

2.2 The Window of Maximum Exposure

The transition period, from the announcement of a reorganisation to vesting day, is the period of highest security and operational risk in a council's history. Several factors converge simultaneously:

- IT teams are stretched between running existing services and planning for the new authority
- Third-party contractor volumes surge, with system integrators, legal advisors, HR consultants, and technology migration partners all requiring temporary access
- Data volumes being moved or copied increase sharply, raising the risk of accidental exposure or deliberate exfiltration
- Supplier and contract rationalisation creates gaps in operational visibility and accountability

©2026 Zscaler, Inc. All rights reserved.

- Staff uncertainty about roles in the new authority creates an elevated insider risk profile

The Local Digital team at MHCLG has noted that cyber security can be 'overlooked in the early planning stages' of LGR, with many councils treating identity, security, and data governance as secondary to system migration logistics.

2.3 Why Traditional Networking Cannot Solve This

The conventional response to the 'give staff access to another organisation's systems' problem is to build network-level connectivity: site-to-site VPNs, firewall rules to permit traffic between IP ranges, and point-to-point links between data centres. This approach has three fundamental problems in an LGR context:

- **Speed:** Provisioning traditional network connectivity between multiple organisations, with all associated change control, firewall change requests, and testing, takes months. LGR timelines do not accommodate this.
- **Cost:** Running multiple parallel network environments, one for each predecessor organisation, through a multi-year transition is expensive. Each environment requires its own operational support, licensing, and security monitoring.
- **Security posture:** Network-level access grants too much. A VPN connection into another council's network grants broad access to that network segment, not just the specific application the user needs. This violates the principle of least privilege and dramatically increases the blast radius of any security incident.

3. The Solution Framework: ZTNA and SSE

3.1 What These Technologies Actually Do

Zero Trust Network Access (ZTNA) replaces the concept of 'trusted network' with 'verified identity'. Instead of granting access based on where a user is (which network they are on), ZTNA grants access based on who they are (verified identity), what device they are using (device health and compliance), and what they are allowed to access (application-level policy). Access is granted per-application, not per-network segment.

Secure Service Edge (SSE) extends this model to cover the full range of security functions a council requires: secure web gateway (controlling internet access), cloud access security broker (governing SaaS application usage), and ZTNA, all delivered from a cloud-native architecture that is not tied to any specific physical location or network.

Together, these capabilities mean that a user's secure, governed access to authorised applications travels with them regardless of which predecessor organisation's building they are in, which network they are connected to, or which device they are using.

©2026 Zscaler, Inc. All rights reserved.

THE FUNDAMENTAL SHIFT:

Traditional model: ‘You are on our network, therefore you are trusted.’

Zero Trust model: ‘You have proven who you are, your device is healthy, and policy permits this access, therefore you may access this specific application.’

In an LGR context: staff from any predecessor organisation, on any legacy network, can access exactly the applications they need from day one.

4. Use Cases: Where This Matters in Practice

4.1 Day-One Staff Access Without Network Convergence

The problem
On vesting day, thousands of staff from dissolved predecessor councils must log in and perform their statutory duties. The new unitary’s unified network does not yet exist. Staff are sitting in buildings that belong to different legacy organisations, on different networks, with different usernames and credentials.

The traditional approach
Federated VPNs between legacy councils, with firewall rules negotiated over months between IT teams. IP addressing conflicts require re-addressing or NAT workarounds. Staff on ‘the wrong’ network cannot access the systems they need. Service delivery fails.

The ZTNA outcome
Staff from any predecessor organisation access authorised applications through an identity-verified, policy-enforced tunnel regardless of which network they are on. No physical network convergence is required before vesting day. Access follows identity, not location.

Strategic value
Avoids the political and reputational disaster of a new council that cannot function on its first day of legal existence. Enables the IT programme to deliver physical network convergence on a rational timetable rather than a crisis timetable.

4.2 Decommissioning Legacy Councils Without Stranding Users

The problem
A dissolved district council’s network is switched off. Former staff who have transferred to the new unitary still need access to legacy case management systems, planning records, and financial archives for months, sometimes years, during transition and for legal retention purposes.

©2026 Zscaler, Inc. All rights reserved.

The traditional approach
Keeping the old network alive specifically to maintain access to legacy applications, which incurs ongoing infrastructure, support, and licensing cost for systems and networks that are no longer operationally necessary, but cannot be switched off without stranding users.

The ZTNA outcome
Access to specific legacy applications is granted via policy through the ZTNA layer, independently of the underlying network. When the legacy application is eventually decommissioned, access policies are revoked centrally. No network infrastructure needs to remain operational purely to support application access.

Strategic value
Accelerates the decommissioning timeline for predecessor IT estates, delivering direct cost savings on infrastructure, support contracts, and licensing. Eliminates the 'zombie network' problem that has afflicted previous council reorganisations.

4.3 The Shadow Authority Operating Before It Legally Exists

The problem
Shadow authorities, elected but not yet legally empowered bodies, need to plan the transition, collaborate on policy, review sensitive data, and prepare operational plans for vesting day. They have no IT estate of their own and no network to operate from.

The traditional approach
Shadow authority members and officers operate informally across multiple predecessor systems, sharing documents via email, using personal devices, and creating an ungoverned environment with no consistent security policy.

The ZTNA outcome
A lightweight, identity-governed access environment can be stood up rapidly without procuring physical infrastructure to give shadow authority members access to a governed, monitored collaboration environment. SSE enforces data governance on what leaves each predecessor organisation into the shared space.

Strategic value
The shadow authority operates securely and effectively from the moment it is constituted. Transition planning is better governed, more auditable, and less likely to create legacy data governance problems that the new unitary inherits on vesting day.

4.4 Governing Data Across the Highest-Risk Transition Period

The problem
LGR creates the conditions for significant data loss, accidental exposure, or deliberate exfiltration. Data from multiple predecessor organisations is being moved, copied, restructured, and migrated simultaneously. Third-party contractors have temporary access to sensitive resident data.

©2026 Zscaler, Inc. All rights reserved.

Staff uncertainty about future roles elevates insider risk.

The ZTNA/DLP outcome

Data Loss Prevention policies, delivered through the SSE layer, classify and govern sensitive data categories, i.e., children's services records, adult social care, housing and benefits data, financial systems, across all predecessor environments from the moment integration activity begins. Policies travel with the data, not the network perimeter.

Strategic value

Protects the new council from inheriting a predecessor's data breach or ICO investigation. Provides the governance evidence trail that the new unitary's Data Protection Officer and senior leadership will need to demonstrate accountability under UK GDPR throughout the transition.

4.5 Managing the Contractor Surge Safely

The problem

LGR triggers a significant surge in external contractor activity: system integrators, legal and HR advisors, IT migration partners, and specialist consultants. Each requires access to council systems from outside, often on unmanaged personal devices, over a period of months.

The traditional approach

VPN credentials issued to contractors provide broad network access that is difficult to scope, audit, or revoke. Different predecessor councils manage contractor access differently, creating inconsistent security posture across the transition programme

The ZTNA outcome

Contractors receive time-limited, application-specific access with full audit trails through the ZTNA layer. They never touch the internal network. Device health checks can be enforced at access time. When a contract ends, access is revoked via policy instantly and completely, rather than through a series of IT tickets that may take days or weeks.

Strategic value

Reduces the risk of a contractor-caused breach during the most exposed period in the council's history. Provides the audit trail required for ICO accountability, procurement compliance, and internal governance reporting.

4.6 Rationalising the Cost of Multiple Security Estates

The problem

Councils undergoing LGR will inherit multiple parallel network security environments: different VPN platforms, different firewall vendors, different endpoint security tooling. Running these in parallel through a multi-year transition is expensive, complex, and creates inconsistent security outcomes across the new organisation.

©2026 Zscaler, Inc. All rights reserved.

The ZTNA/DLP outcome

A single cloud-native SSE platform replaces the need to maintain multiple VPN and firewall environments. Legacy network security infrastructure can be retired on a managed timetable rather than maintained indefinitely. Research from previous reorganisations has identified that long-term savings are found specifically in consolidating infrastructure and reducing duplicated systems.

Strategic value

A direct, quantifiable cost saving that can be presented in the business case for digital investment. ZTNA is not an additional cost on top of existing infrastructure: it replaces infrastructure that would otherwise have to be maintained across multiple predecessor environments for the duration of the transition.

4.7 Protecting Staff Experience Across Dispersed Legacy Buildings

The problem

Staff from former district and county councils will continue working from legacy buildings for years, under a new employer, on networks that are not yet unified. Degraded application performance and broken access are not just operational inconveniences. Rather, they are visible, daily evidence that the merger is not working, affecting staff morale, retention, and ultimately service quality.

The ZTNA + Employee Experience Monitoring outcome

Application performance and access reliability can be monitored and assured across every legacy location and network simultaneously. Leaders receive visibility into where staff productivity is being impacted by technology performance, and can act before degraded experience becomes a staff retention issue or a union grievance.

Strategic value

Staff experience directly affects public service delivery. A council leadership team that can demonstrate with data that the reorganisation has not degraded service quality is in a substantially stronger position with residents, elected members, and central government.

4.8 AI Governance Across Inherited Environments

The problem

Staff across predecessor councils have been using a patchwork of AI tools: Microsoft Copilot in some, various SaaS AI products in others, with unsanctioned ‘shadow AI’ usage present in most. The new unitary inherits unknown AI data exposure across multiple environments, with no consistent governance framework. Sensitive resident data may already have been processed through uncontrolled AI services.

The SSE/AI Security outcome

An SSE layer provides visibility and control over AI tool usage across all user populations, regardless of which legacy network they sit on. A single, consistent AI acceptable use policy can be established and enforced from day one of the new authority before the internal network is unified.

©2026 Zscaler, Inc. All rights reserved.

Strategic value
Avoids an ICO investigation or data breach caused by an inherited AI governance gap. Demonstrates to central government, residents, and elected members that the new council has approached data stewardship responsibly from its inception.

5. Use Case Summary

Scenario	Strategic Risk Without Action	Outcome with ZTNA / SSE
Day-one staff access	New council cannot function on vesting day. Statutory service failure.	Staff access authorised applications via identity, not network. Works from day one across all legacy environments.
Decommissioning legacy networks	Predecessor networks kept live at ongoing cost to maintain application access.	ZTNA decouples access from network. Legacy infrastructure retired on a rational timetable.
Shadow authority operations	Ungoverned, unauditable collaboration across personal devices and informal channels	Secure, governed shared environment stood up rapidly without physical infrastructure.
Data governance during transition	Data breach or ICO action caused by uncontrolled data movement across merging organisations.	DLP policies travel with data, not the network perimeter. Consistent governance from day one.
Contractor access surge	Broad VPN access to thousands of temporary contractors. Difficult to scope, audit, or revoke.	Application-specific, time-limited, audited access. Revoked instantly on contract end.
Network security estate rationalisation	Multiple parallel VPN and firewall environments maintained at significant ongoing cost.	Single cloud-native SSE platform replaces multiple legacy security estates. Direct cost saving.
Staff experience across legacy sites	Degraded performance visible to staff daily. Morale, retention, and service quality impacted.	Monitored, assured application delivery across all legacy locations. Leadership visibility with data.
AI governance	Inherited patchwork of unsanctioned AI tools. Unknown data exposure. Regulatory risk	Unified AI governance policy enforced across all user populations from vesting day.

©2026 Zscaler, Inc. All rights reserved.

6. The Business Case

The investment case for ZTNA and SSE in an LGR context is built on three pillars:

6.1 Cost Avoidance

Previous reorganisations have demonstrated that councils face 'unexpected costs related to IT migration, licensing, and cybersecurity upgrades' when they do not plan the digital transition carefully. ZTNA and SSE reduce the cost of:

- Building and maintaining temporary site-to-site VPN connectivity between predecessor organisations
- Keeping legacy network security infrastructure operational solely to maintain application access during transition
- Remediating security incidents caused by expanded, ungoverned access during the transition period
- ICO enforcement action resulting from data governance failures during data migration and consolidation

6.2 Cost Replacement

ZTNA is not an additional layer of spend. It replaces the following costs that councils would otherwise carry:

- **VPN infrastructure:** hardware, software licences, and operational support across multiple predecessor environments
- **Firewall estate:** rules management, change control, and vendor support across multiple organisations
- **Perimeter security tooling:** on-premises security appliances that become redundant as services migrate to cloud

6.3 Risk Reduction

The reputational and financial consequences of LGR transition failures are substantial. A council that:

- Cannot provide services on vesting day faces immediate political fallout and potential ministerial intervention
- Suffers a data breach during transition faces ICO enforcement action at a moment of maximum public scrutiny
- Fails to deliver the efficiency savings promised in its reorganisation proposal risks its funding settlement and relationship with central government

ZTNA and SSE directly reduce the probability of all three outcomes.

©2026 Zscaler, Inc. All rights reserved.

7. Conclusion

Local Government Reorganisation is the largest structural change to English councils in over 50 years. It creates a specific, time-bounded, and predictable set of technology and security challenges that traditional network-centric approaches cannot address at the pace and scale required.

ZTNA and SSE are not new or unproven technologies. They are the architecture that has replaced VPN-centric remote access across the private sector, precisely because they solve the problem of giving the right people access to the right applications: regardless of network topology, physical location, or organisational boundary.

Applied to LGR, they deliver four things that council leaders need above all else: services that work on vesting day; a transition period that does not create catastrophic data or security risk; a clear path to cost reduction through infrastructure rationalisation; and the governance visibility to demonstrate accountability to residents, elected members, and central government.

The question for councils is not whether they will face these challenges. They will. The question is whether they address them with an architecture designed for the problem or attempt to solve a 2027 problem with infrastructure designed in 2005.

About Zscaler

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform. Learn more at **zscaler.com** or follow us on Twitter **@zscaler**.

© 2026 Zscaler, Inc. All rights reserved. Zscaler™ and other trademarks listed at **zscaler.com/legal/trademarks** are either (i) registered trademarks or service marks or (ii) trademarks or service marks of Zscaler, Inc. in the United States and/or other countries. Any other trademarks are the properties of their respective owners.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com**

zscaler™

Act Fast.
Stay Secure.