Local Government Reorganisation: The Outcomes Case for Zero Trust

What every Chief Digital Officer, CDIO, and digital leader needs to know before vesting day

PROGRAM BRIEF

England is replacing hundreds of county and district councils with new unitary authorities by April 2028. For most areas, this means multiple organisations, each with their own people, IT systems, data, and security models, must merge into one and be fully operational from a single legal vesting date. There is no option to delay, no grace period, and no tolerance for failure in statutory services. This is the biggest public sector M&A programme in 50 years, and digital leaders own the most complex part of it.

The three outcomes you must protect against

1. Service Failure	2. Data Breach	3. Cost Overrun
If staff cannot access the systems they need on vesting day, because they sit on a legacy network with no connection to the new authority's environment, statutory services fail. Planning, housing, social care, benefits. Publicly, immediately, and with ministerial consequences.	The transition period is the highest-risk period in a council's data history. Data moves across organisational boundaries. Contractor numbers surge. Staff uncertainty is elevated. Without consistent, enforced data governance, the new council inherits its predecessors' exposure.	Maintaining multiple parallel IT environments, one per predecessor organisation, through a multi-year transition is expensive. Previous reorganisations produced unexpected costs in IT migration, security upgrades, and infrastructure that was kept live solely because switching it off would strand users.

Why Zero Trust changes the equation

Traditional IT connects people to networks. Zero Trust connects verified people to specific applications: regardless of which network, building, or organisation they sit in. In an LGR context, this distinction is everything.

Instead of spending months building VPN tunnels between predecessor organisations, managing conflicting IP addresses, and negotiating firewall rules across IT teams that are already stretched, a Zero Trust architecture lets you:

- Give staff from any predecessor organisation access to any authorised application on day one of the new authority, without waiting for physical network convergence
- Retire the predecessor networks on a rational timetable rather than keeping them alive at ongoing cost purely to maintain application access

- Apply consistent data governance across all merging organisations from the moment integration begins, not after the network is unified
- Give contractors time-limited, application-specific access that is revoked automatically, with a full audit trail for ICO accountability
- Monitor application performance and staff experience across all legacy sites, so you can demonstrate to senior leaders and elected members that the transition is not degrading public services
- Enforce a consistent AI governance policy across all inherited environments from vesting day

THE CONVERSATION THAT MATTERS

The question is not 'should we buy a security product.' The question is: 'how do we ensure our new council cwan operate from day one, manage a 2-to-3 year transition without a catastrophic breach or cost overrun, and emerge with a modern, cloud-native architecture rather than a collection of stitched-together legacy environments?'

Zero Trust Network Access and Secure Service Edge answer that question more directly, more cost-effectively, and with less operational risk than any network-centric alternative.

What good looks like by vesting day

Without Zero Trust	With Zero Trust
Staff on predecessor networks cannot access new systems on vesting day	All authorised staff access all authorised applications from day one regardless of location
Legacy networks kept live at full cost for 2–3 years to avoid stranding users	Legacy infrastructure retired on a planned schedule; access decoupled from network
Thousands of contractor credentials issued with broad, ungoverned access	Contractors receive scoped, time-limited, audited access revoked automatically on exit
Data governance breaks down as data moves across organisational boundaries	Consistent DLP policy enforced across all environments from the start of integration
IT teams manage multiple parallel security estates with inconsistent policies	Single policy layer across all inherited environments; one control plane, one audit trail

©2026 Zscaler, Inc. All rights reserved.

Zero trust and the integration life cycle

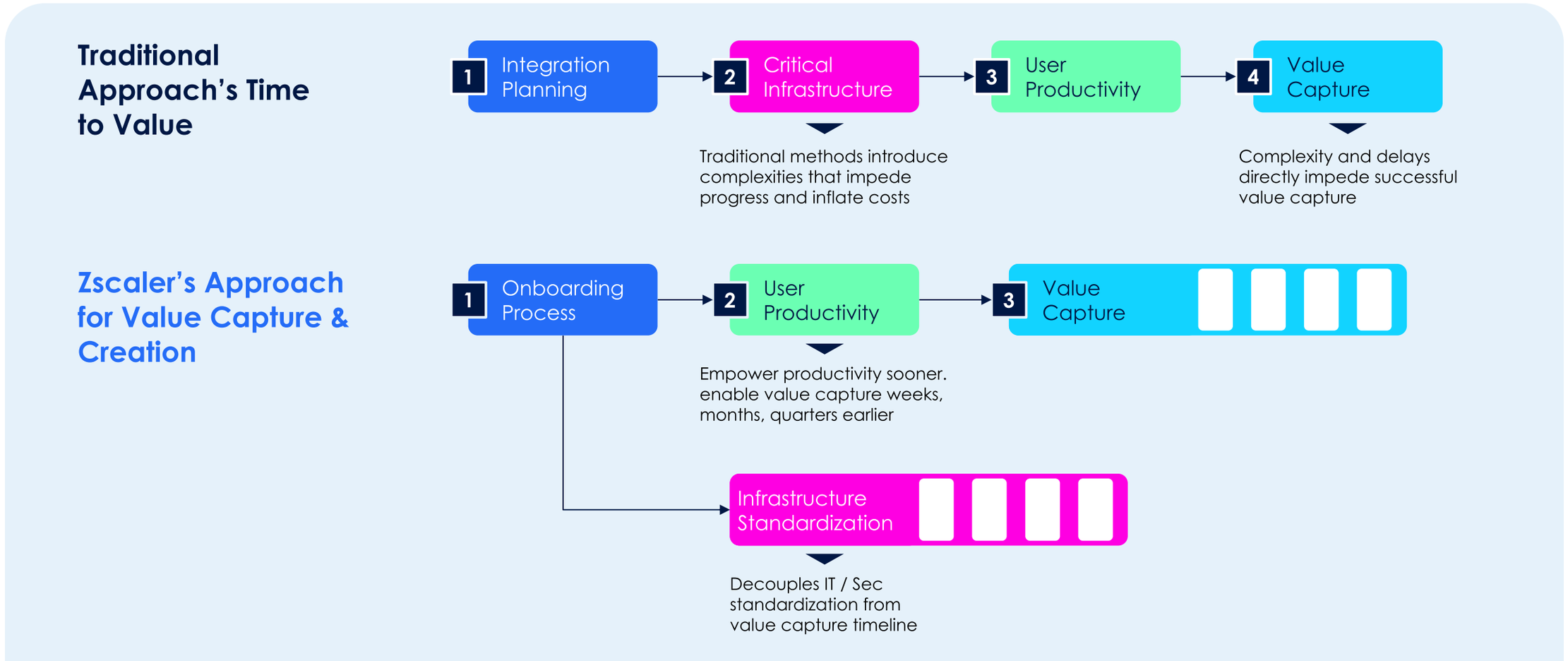
Day 1: Integration

- Connect resources across your organisation with no need to address underlying network complexity: get users productive on Day 1
- Contain acquired vulnerabilities or potential compromises instantly when you overlay your risk posture on the acquired network
- Deliver seamless access to any cross-organisation apps and resources with a simple desktop agent

Day 2 and Beyond: Optimization

- Expand and fine-tune Day 1 deployment as you transform to a zero trust architecture
- Connect and secure users and data anywhere while greatly reducing technical debt
- Achieve synergy savings targets with lower run-rate costs by eliminating hardware refresh cycles, support contracts, network circuits, and more

How to integrate on a value driven timeline



Transition from Integration Project to Onboarding Process

"Integrate" on a Value Driven Timeline

- Rethink of Day 1+ as an onboarding any entity. Provide near instant secured cross-entity access with no deployment or disruption to either side
- Allow the integration / standardization to run in a parallel workstream with confidence

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**.

© 2025 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™

Experience your world, secured.™