Data Sheet

Mitigate Cyber Risk While Simplifying a Machinery of Government Change

The reality of machinery of government (MoG) is significantly stressful for agency leaders, CIOs, and network architects responsible for a successful IT integration. MoG changes are often high-profile events and must be implemented as quickly as possible, with as little fuss as possible, so that the new agency can deliver on its commitments to citizens, faster.

A MoG change can also serve as a catalyst for modernisation. It is an opportunity to consider new technologies for standardisation across multiple agencies and ensure a seamless experience for all users.

As agencies across government look to embrace modern, cloud-based technologies to support their mobile, work-from-anywhere workforce, the concept of a 'zero trust' approach to the connection of users to resources, machines, and applications has come to the forefront of modern IT thinking.

This paper describes the challenges a CIO faces during a MoG and provides advice on how a contemporary zero trust network integration approach enables speed and agility to the MoG change process.

Part 1

Machinery of government change: challenges and advice for the CIO

The election is over and the MoG change has been announced. Little if any planning has been done upfront. You need to integrate or separate different systems and technologies applying an inconsistent mix of policies and procedures. Changing gears from the previous state of dealing with efficiency dividends and keeping things running smoothly, you now have to meeting new set of expectations in a minimal time frame. The Minister expects instant access and productivity. The entire organisation is looking at you to keep them up and running. There are generally two sides to every MoG: one side sees parts of the current organisation being removed, and the other sees their organisation growing. The unfortunate reality is many

departments see both happening at the same time.

If you can integrate the new agencies and separate the jettisoned agencies quickly and effectively, you can have a positive effect on the overall success of the new government's agenda. However, if this is a long, drawn-out process, you could be responsible for issues both practical and political.

Through the course of this change, productivity levels are challenged and security risks are often overlooked or even ignored. As agency leaders often remind us, the job of the CIO is to enable productivity, reduce cost, and deliver effective citizen services.

CIOs need a playbook in hand on day zero to effectively manage the first 90 days and limit the long tail of IT integration that follows a MoG. Larry Biagini, chief technology evangelist at Zscaler, draws on his experience as the former CTO of GE to outline four steps CIOs must take for effective IT integration.

1. Communicate

Employee engagement often dips following the announcement of a MoG. It is paramount to be transparent and open to continue fostering trust. While functions may have been merged or separated, the agency won't want to pause for you to get up and running. In the first few days, it's crucial for communications to flow seamlessly between teams.

Agencies affected by a MoG are hotbeds for rumour and innuendo. By integrating major communications channels and working effectively with IT teams, both old and new, you can ensure everyone has timely access to accurate information and is working collaboratively. Granted, there are bound to be some issues in the integration process. But the typical workforce knows this; all they need is evidence that the decision-makers are responding to it in one form or another.

2. Assess your risk

What new risks is the agency bringing in—financial, operational, security? After the merger/separation, it's important to carefully evaluate the environment to measure the impact and likelihood of any and all risks.

The minute you merge or separate, your risk profile goes up, both from a security and compliance perspective as well as from a financial perspective. The agencies involved will have different vulnerabilities, gaps, and priorities to realign. There may be long-term contractual commitments that inhibit the ability to align, or a changed regulatory and legislative compliance requirement introduced as a consequence of the changes.

Of all these matters, the first you need to assess is security. A breach of any size can have a direct negative practical and political impact—not to mention it is easier to attack an organisation in flux using methods like phishing attacks and identity theft.

There is also an increased risk of intentional or unintentional data leakage, the insider threat, the disgruntled employee. As such, organisations need to develop and execute a security strategy as soon as a MoG change takes place.

3. Integrate the players

In the first few days, the CIO needs to really touch all parts of the newly combined organisation to make sure all players feel like they're valued and integrated—and that they will be evaluated and promoted based on their merits, not which agency they were in. Strong people often see a merger as an opportunity to move up or move on. Your job as CIO is to influence that choice early in the situation to keep as many strong players on your team as possible.

4. Yours, mine, or ours?

The cloud changes everything, and CIOs need to leverage that transformation in their planning. As you face the potentially daunting task of assessing which distinct aspects and technologies of each organisation should be retained, it's worth considering the benefits of throwing out the legacy products of both companies and using the merger/separation as an opportunity to accelerate the transition to the cloud, reduce capital costs, and streamline processes.

IT consolidation is constantly happening in the private sector, driven by mergers and acquisitions. This has a significant impact on the brand and customer experience. Senior executives and boards rely on the IT executive to be decisive in selecting a technology stack that will shape their new company's future. Very similar forces are at play in the public sector, with governments seeking to promote their policy priorities post-election. Knowing this, starting early and being decisive is critical. Private sector M&A is generally well considered, and before decisions are made to acquire or separate, detailed plans are prepared to understand the time and cost of the transition as well as prove the underlying business case. This level of detailed planning is not a regular feature of the MoG process.

In today's political climate, it's not a matter of if you will be involved in a machinery of government change, but rather when. Will you be ready?

PART 2

Simplifying and accelerating machinery of government changes through zero trust

Zscaler brings speed and agility to a MoG through the Zscaler Zero Trust Exchange™. The platform enables agencies to act on savings opportunities and synergies earlier. Zscaler reduces the usual ICT integration timelines while offering options on the level of integration or separation of organisations. This enables agencies to showcase the 'quick win' collaborations and gain the confidence of government stakeholders and citizens.

After the MoG is announced, we begin a structural process dreaded by many IT teams: connecting two disparate agency infrastructures into a cohesive unit. This means long hours, costly process creation, and complex patchwork to provide both sets of users with cross-agency connectivity. If only there were a simpler and more efficient way to accomplish these goals. There is: zero trust network access (ZTNA).

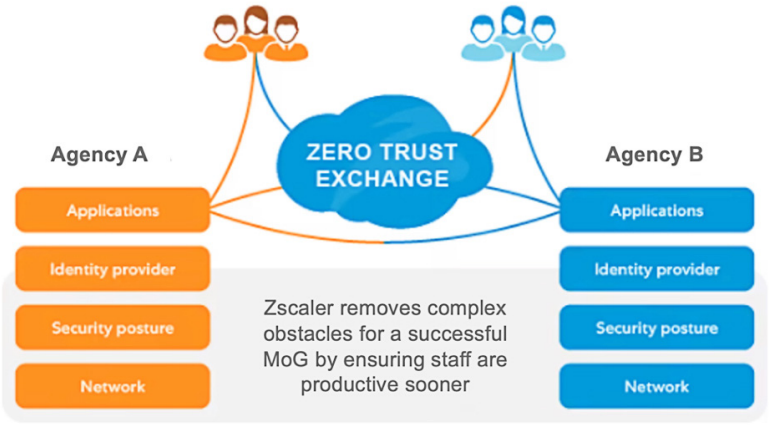

Figure 1: Simplified MoG with the Zero Trust Exchange

Merging legacy systems? Complex, expensive, risky, slow...?

The purpose of the MoG change is to combine resources for two (or more) agencies to advance defined citizen service delivery goals. What often gets in the way of resource availability is access. Different agencies use different networks, architectures, and systems to host and distribute resources to their workforces. One of the first CIO priorities during and after a merger is providing easy and—more importantly—secure access to newly acquired or merged data, infrastructure, and applications to staff.

In a perfect world, all MoG affected agencies would come with a straightforward and complete integration plan. Flip a switch, and employees, systems, applications, networks, data centres, and facilities synchronise automatically, with no hassles. If only it were ever that simple. Some organisations create dedicated teams and draft playbooks to standardise integration activities, all to realise the benefits of the MoG change sooner.

Full system integrations can be extraordinarily complex and—thanks to unanticipated scope creep—more expensive than the initial assessment suggested. Cost-constrained parent agencies stretch integration out over an extended timeline, ranking system importance and prioritising the integration process in phases. In the meantime, employees are left to fend for themselves with disparate, isolated systems that don't necessarily enable cross-communication between users. And the integration phases that do move forward have to fight for resources with competing priorities and initiatives.

This ad hoc integration approach rarely yields an acceptable outcome. The cost of integrating legacy technologies into a cohesive network is a nightmare to estimate and contain. Yearly budget refresh cycles often don't take this integration into account, and the money allocated for updating hardware, systems, and applications isn't sufficient for one agency (let alone two or more).

This leads to ongoing maintenance and security efforts for multiple disparate networks—which is its own cost and resource nightmare.

Agencies attempting to integrate legacy network and security infrastructures often resort to 'creative' ways to get users' access to resources in disparate networks—temporary fixes that could poke holes in firewalls and secure access protocols. And with these temporary fixes come increased security concerns, user issues, and troubleshooting nightmares for IT. Operation teams spend countless hours trying to identify and resolve issues due to the network address translations (NAT), routing, and firewall rule manipulations.

Zero trust network access: rapid asset access

Fully integrating two legacy networks can be a costly and time-consuming process. The traditional approach is for IT teams to provide employees with VPN connectivity. These VPN connections work, but they strain network resources—especially as the number of VPN users climbs. Worse, the increased VPN connections extend both networks' attack surfaces.

VPN access is a poor substitute for direct connectivity. Managing it is costly, and VPNs introduce risk. And of course, dealing with more than one agency at a time further complicates these issues. The VPN approach produces gaps in security. So, how can you avoid incurring that risk? The (unintuitive) answer is to not converge networks in the first place.

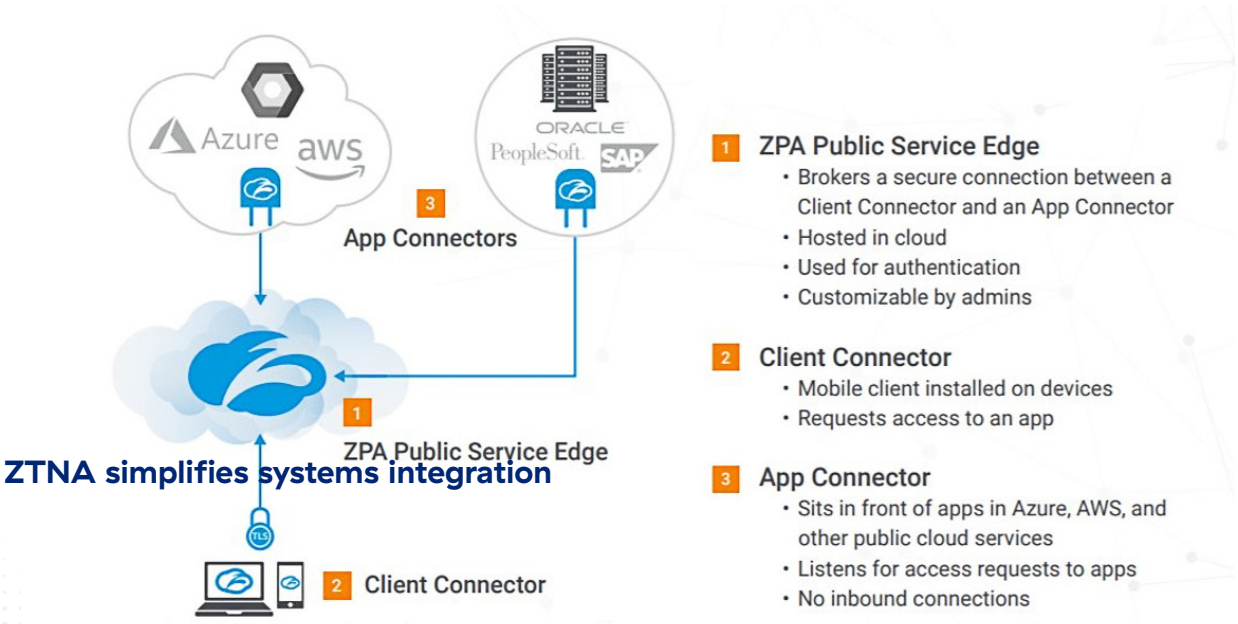

Figure 2: Zero trust architecture

ZTNA simplifies systems integration

ZTNA is a contemporary alternative. An agency adds traffic forwarding connectors to each network data centre and a software agent to each user's device, and then creates policies that allow users to connect to the applications they need, accessible from either network, wherever users connect.

ZTNA uses policies to authorise user access to applications and networks. ZTNA accelerates MoG time to value, providing cross-agency connectivity for users in weeks rather than months or years (or never).

ZTNA is a set of technologies that operates on an adaptive trust model: trust is never implicit, and access is granted on an identity-based, least-privileged basis as defined by granular policies. ZTNA gives users seamless and secure connectivity to applications without ever exposing the network, applications, or data to the internet. Connectivity is direct, delivered via distributed cloud services, and accessible from anywhere. In this way, ZTNA can ultimately supplant an agency network with outdated perimeter security.

Unlike network-centric solutions like VPNs or firewalls, ZTNA takes a fundamentally different approach to securing access to internal applications based on four core principles:

1. **ZTNA completely isolates the provisioning of application access from any requirement for network access.** This isolation reduces risks to the network, such as infection by compromised devices, and only grants application access to authorised users.

2. **Cloud-enabled ZTNA offers outbound-only connections ensuring both network and application infrastructure are made invisible to unauthorised users.** IP addresses are never exposed to the internet, creating a "darknet" that obscures internal resources from unauthorised view.

3. **ZTNA's native app segmentation ensures that once users are authorised, application access is granted on a one-to-one basis.** Authorised users have access only to specific applications, rather than unfettered access to the full network in a legacy environment.

4. **ZTNA takes a user-to-application approach rather than a network-centric approach to security.** The network becomes de-emphasised, and the internet becomes the new corporate network, leveraging end-to-end encrypted TLS microtunnels instead of MPLS.

With ZTNA in place, you may never need to bother with full acquired-agency-infrastructure integration.

Managing user access to authorised applications (governed by user and app-centric policies) provides application segmentation without requiring network segmentation. Once a user is added to a policy and application authorisation is granted, a user can gain access to an application on either network without requiring the networks to be connected.

Managing integration complexities like IP address remediation and circuit overlaps isn't trivial: merging networks is complicated, time-consuming, prone to error, and expensive.

ZTNA provides immediate access to internal resources for joined organisations. If, for whatever reason, a parent agency still wants to integrate acquired infrastructure, that work can be conducted behind the scenes and without the same urgency, since users already have access to necessary resources/applications. With the proper planning, systems can be included in the budget planning cycle and then migrated during refresh either to an enterprise data centre or the cloud.

Access is better today than tomorrow (or next year)

ZTNA never inherently trusts anyone from inside or outside the network until verified. ZTNA removes the distinction between 'inside' and 'outside' since connectivity is secured between the user and application. Security is not based on gateway access through a secured network perimeter. Access to internal business systems or applications can be granted only after authorisation. Network access is not required, and applications are masked from the open internet.

After a MoG change, ZTNA allows IT teams to focus on integrating data, systems, and applications on their own terms, where and however it best meets the business's needs. In the meantime, workforces from each agency can access whatever resource they need, wherever it may be, and from wherever they may connect without complex network integrations, without VPN security exposure and resource use, and without expensive retooling of network architectures.

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