CIO JOURNEY

Kelly Services

A Blueprint for Secure Cloud Transformation

Company:	Kelly Services	**Revenue:**	$5.5 billion
Sector:	Workforce Augmentation	**Employees:**	10,000
Driver:	Darryl Staskowski	**Countries:**	22
Role:	SVP & CIO	**Locations:**	870

Company IT Footprint: In 2010, when Kelly Services first started its transformation journey, it was supporting over 10,000 employees across 870 locations in 22 countries. This infrastructure was supported by 17 different MPLS network providers. By the time Kelly Services completed Phase 1 of it transformation journey, it had reduced its MPLS footprint from 870 locations to 30 with the help of SD-WAN services.

"The cloud transformation journey is to a simpler, more effective, more resilient IT infrastructure. Taking a phased approach will reduce disruption to operations, while generating the cost savings that can fuel each new phase."

Darryl Staskowski, Senior Vice President and Chief Information Officer, Kelly Services

Excerpt from: Stiennon, Richard "CIO Journeys" *Secure Cloud Transformation: The CIO's Journey*. IT-Harvest Press, 2019, pp. 153-166.

Kelly Services Journey Overview

Business Objectives

- Reduce network complexity, costs (MPLS, branch NGFWs)
- Deploy Office 365
- Eliminate WAN congestion
- Improve branch-office user experience

The Solution

- Culture — Evangelize, Engage, Plan:
  - Identify champions, get senior exec buy-in
  - Build a culture of risk-taking, empowered decision-making
- Five phases:
  - Migrate to Office 365
  - Local internet breakouts for web traffic
  - Local internet breakouts for ALL traffic
  - Move internal apps to cloud
  - Optimize connectivity, app access

Impact

- Reduced CAPEX: $4M annual on appliance sprawl
- Reduced OPEX: $2.7M annual on management costs
- Widespread adoption across 900+ offices, 22 countries
- Local internet breakouts mean "the new perimeter is identity."
- Better user experience, particularly at branch offices
- Elasticity: Cloud firewall scales by user, not bandwidth
- Bandwidth control prioritizes Office 365 over YouTube

Darryl Staskowski is the SVP and CIO at Kelly Services, one of the largest workforce augmentation companies in the world. The company has followed a strategy of growth through acquisitions in countries in the major regions, which led to a globally disparate set of networks and applications. Kelly Services went through a five-phase cloud transformation journey. Darryl shares his experiences next on how cloud transformation helped his organization deliver solutions that created a better user experience and enhanced business agility.

In the words of Darryl Staskowski:

The pre-transformation state

In 2010, we had 870 locations in 22 countries supported by 17 different MPLS network providers at Kelly.

With data centers in three major regions and separate disaster recovery data centers for backup, our architecture had grown into one which is similar to many large organizations today.

Each data center was protected by a different set of legacy appliances. They had next-gen firewalls from three different vendors and proxy devices, all managed by separate regional teams aligned with each business unit.

Business needs drive transformation

But architectures don't drive change, business needs do. And in our case, it was the lack of consistent collaboration tools among the divisions and regions that brought home the realization that change was required. We wanted our executives and teams around the globe to be able to use the same tools for collaboration, video, and document sharing, and have the same experience when it comes to availability and performance, no matter where they were.

Our IT teams were so busy addressing issues with so many different systems that new IT projects, such as rolling out Wi-Fi to each office and deploying common collaboration tools, were not getting done.

On top of that, the overall posture of the organization was in an unknowable state. All those networks were difficult to manage. There was no way to ensure that security policies were constantly enforced across all these devices. We were starting to be faced with significant capital expenditures and continued operational expenditures just to keep doing business as usual if we didn't make a change.

> *“Our transformation journey followed five phases, which started with a focus on a network purpose-built for leveraging the SaaS applications.”*

The Five Phases of Our Transformation Journey

We knew that cloud transformation would deliver solutions that helped create a better experience for our users, help us reduce business risk while enhancing our business agility, and provide us a competitive advantage, all while reducing our total cost of ownership (TCO).

Our ideal reference architecture could simply be defined as a cloud layer that connects all users to all applications, based on business policy, with a consistent end-user experience, no matter where users are or what device they are using—all at lower cost, while being simple to manage.

This is all that our internal architects needed to start our cloud transformation. The process for us at Kelly Services started with applications moving to the cloud. Our transformation journey followed five phases, which started with a focus on a network purpose-built for leveraging the SaaS applications the business demanded, while creating an enhanced infrastructure posture at a lower TCO. Once the branch network was complete, the focus shifted to moving data center workloads to IaaS and delivering a consistent end-user experience for access to all business systems, regardless of where they were hosted.

Phase 1. Migration to Office 365

The first step for us was to standardize on a single email and business productivity suite. We chose Microsoft’s Business Productivity Online Suite (BPOS). BPOS was an early version of Microsoft Office 365. Moving the entire organization to Office 365 accomplished much of the collaboration experience that we needed with SharePoint, and the rest of the suite adding to their capabilities.

We also moved to a standard firewall platform in each of our global data centers managed by a single MSSP. We deployed 24 additional firewalls to sites with more than 80 people, so we could achieve local breakouts for internet access.

In this phase, we also consolidated carriers by awarding a single contract for global network services. This consolidation reduced the MPLS footprint from 870 locations

to 30 with the help of SD-WAN services, where most office traffic was delivered to an MPLS backbone via an IPsec tunnel over the internet.

The next step was to eliminate utility services in each office. DNS and Active Directory Domain Controllers were consolidated into data centers. Print and file servers were also moved. Now, the IT services in the remote offices were simplified. Just end-user devices and LANs had to be managed.

The end state after Phase 1:

- Nine data centers with MPLS-only connectivity. All internet traffic from branch offices backhauled to the data centers before being routed to the internet.
- 24 locations with MPLS circuits and internet protected by UTM security appliances managed by a single service provider.
- There were 870 small offices with local internet connections and perimeter devices to terminate IPsec tunnels into the MPLS backbone. Note that the internet was used as transport, but local breakouts were not enabled. Traffic to the SaaS applications still went to the MPLS backbone first, where it then went through the regional data centers.
- Consolidated utility computing (DNS, file, and print servers) to data centers.

These changes created cost savings that funded the remaining phases of our transformation. The networking changes alone saved 60% from our budget for MPLS circuits. It also created a better internet experience for those in the regional and country headquarters, where UTM appliances were deployed. Our IT operations were vastly simplified with common email, SharePoint, and a single MPLS and SD-WAN provider.

Phase 2. Local breakouts for web traffic at all locations

In the next phase, we embarked on a project to introduce local internet breakouts to 870 small offices, so we could take advantage of Skype and SharePoint Online and any SaaS application or online resource.

This was done using the Zscaler cloud security service for web traffic for ports 80 and 443. PAC files were pushed to personal computers that were deployed in each office. Zscaler maintained a global PAC file that used geolocation to determine which Zscaler global data center was the most appropriate for security and policy enforcement.

Providing connections to Office 365 is challenging for any organization. More than 700 separate rules were required, because the branch devices did not support domain name rules, and applications like Skype require more than just ports 80/443. Every time Microsoft provisioned new IP address ranges for its services, the SD-WAN device configuration needed to be updated.

Phase 3. Local Breakout of all internet traffic

The next phase we embarked on was to build full VPN IPsec tunnels from each branch office to the Zscaler cloud for all internet bound traffic. Zscaler essentially became the default route to the internet. Our network service provider provisioned very simple routers at each of our offices that could send internet traffic to the nearest Zscaler data center and internal traffic to our corporate data centers through tunnels that reached the MPLS backbone. The branch router or SD-WAN device were very simple to manage as there were no complicated rule sets to be enforced.

Now, all traffic over all ports and protocols was being routed to Zscaler, taking advantage of its full Cloud Firewall capability. Instead of the more than 700 policies that were required, all our offices had a common set of only 12 policies.

At the same time, the requirement for managing the firewalls at our larger offices was reduced considerably, thanks to the Cloud Firewall service.

Application prioritization for Office 365 traffic

Office 365 posed a bandwidth problem for us at Kelly. It was a critical application, so it needed guaranteed performance and responsiveness, but at the same time, because OneDrive started to replace the local file servers, file transfers could bog everything down. By implementing bandwidth controls available within Zscaler,

> *“End users should not be the ones making decisions about how they connect to IT resources.”*

Office 365 could be guaranteed 30% of all bandwidth, but also be limited to no more than 50%, so that other apps continued to work effectively.

A lesson learned during this phase was that end users should not be the ones making decisions about how they connect to IT resources. Many were still launching their VPN client when they were connecting to Office 365 applications, leading to performance issues. The choice of connectivity should be solved by technology, not the end user.

This phase delivered a consistent end-user experience across our entire network no matter where our users were located. It simplified our overall architecture dramatically, as every user was protected all the time.

Phase 4. Internal application migration to the public cloud

Once our network configuration was architected to provide consistent, secure access to applications, the next phase could begin—migration of our applications to the cloud to improve delivery and resiliency. By moving customer-facing applications to Azure or AWS, we could begin to consolidate our data centers, while improving the experience of mobile workers.

Tight integration between Office 365 and Azure

A bake-off was performed between AWS and Azure. Our team initially picked AWS, because there was a more mature marketplace of options to select from like virtual load balancers and firewalls, but it was Azure’s tight integration with Microsoft and Office 365 that was the deciding factor. We moved customer-facing applications to Azure, with the goal of making them available to our end users without requiring the use of legacy VPN clients.

Attempt to securely access public cloud applications with virtualized security appliances

To protect our applications, we made an attempt to build the same sort of legacy infrastructure that had existed in our data center. Virtualized instances of load balancers and next-gen firewall appliances were deployed in front of the applications. This setup became prohibitively expensive, as scaling these solutions to support more

> *“We made a critical decision not to deploy legacy remote access solutions in the new data center.”*

applications in the future required more and more licenses. It was unsustainable and became hard to justify a business case that actually made it more expensive to host applications in the cloud than in legacy on-premise data centers.

We consolidated four of our data centers in the Asia-Pacific region to one, which reduced the number of sites managed by the third-party MSSP. Meanwhile, our North American data centers were soon to be migrated to state-of-the-art third-party hosting environments.

Phase 5. Secure and fast access to internal applications

We kicked off a *Kelly Anywhere* mobile workforce program, and volunteers were moved away from legacy desktop collaboration spaces to next-generation collaboration spaces hosted in cloud environments. The project was deemed a success, because it provided a consistent user experience for application access, both inside and outside offices.

In this final phase of cloud transformation, we are developing a long-term plan to leverage software defined perimeter (SDP) principles to deliver a consistent end-user experience, regardless of where the application is hosted or where the user is located. Investments in technology are being made to enable future mobile workforce programs, M&A consolidation projects, and as a reference architecture for a future zero-trust network model.

We made a critical decision not to deploy legacy remote access solutions in the new data center. Instead, Zscaler Private Access (ZPA) is being deployed. This cloud-built application access layer integrates with Active Directory and connects authorized users to their applications with no additional hardware or technology in the data center or in front of the applications in Azure.

We leveraged the SDP solution as a new playbook for mergers and acquisitions. The business side has stressed that fast onboarding of new employees after an acquisition was critical, as well as the quick spin off in a sale. Instead of focusing on integrating two networks, it was decided that ZPA would be rolled out to provide

access to required applications for future M&A activities. Policies that only allow specific users to access specific applications can be quickly deployed.

A transition plan was established to move the network to a zero-trust stance long term. Only users coming from the SDP would be granted access to the data centers. The plan was worked into the continuing operations plan by scheduling switch-overs as offices moved their locations (as they did on average every three years) or when internet connections needed to be upgraded.

The move to SDP would free up IT resources that had been focused on the day-to-day challenge of securing 900 branches. In the future, we will be able to focus on improvements in the data center and IaaS platforms. The vastly simplified access control lists (ACLs) in the data center just have to provide for SDP connections.

The results of a phased approach

Our cloud transformation journey is to a simpler, more effective, more resilient IT infrastructure. Taking a phased approach will reduce disruption to operations, while generating the cost savings that can fuel each new phase.

The new perimeter is identity. The location of the users and the applications they need is no longer a concern. A focus on identity and protecting the data center is more cost effective and a better use of resources.

Transformation timeline

The total time frame for network transformation is dependent on a number of variables. For instance, an organization with 60 locations all on one service provider could move to a cloud-enabled network architecture in four to six months. An organization with 900 locations and multiple service providers could take between 12-18 months.

“The new perimeter is identity.”

Other variables include:

Contractual terms of current providers. Companies using multiple providers globally may wait to move to new architectures as their current contracts expire to avoid significant penalties.

Is it a project or a program? You will want to have seasoned project managers that can communicate the status of the project to both internal IT and business stakeholders. Communicate the value of the project with the business—don’t just treat the project like a standard upgrade where you do it during a maintenance window during a holiday or weekend and not tell anyone.

Size of team working on deployment. Most organizations will not have a dedicated team to deploy the new architecture and it will fall either on the Network Operations or Network Engineering teams that are also responsible for other tasks. If that is the case, start with deploying new architecture and configurations as you have to touch each location (example, when a branch office moves). Then implement a process to move a small number per week on top of daily operational duties and start to increase that number as the various teams become more comfortable with the work.

What applications are moving to the cloud? Are they just email, legacy business systems, Salesforce? In some cases, the migration of business systems or adoption of new cloud-based tools will drive business process changes. The deployments can be dictated by the pace at which the business processes change to leverage the new tools.

Lessons learned: what worked well and what didn’t

1. Leverage an ISP aggregator.

- Find a company that can deliver and manage local broadband internet connections at your locations. You want to leverage local providers as you will get the most bandwidth for the cheapest cost.
- You don’t want to have to manage dozens of internet providers. Find one that you give a street address of your location to and they provide the options.

- Ideally you will want more than one internet connection from different providers at your critical locations for redundancy.
- Buying internet from the large service providers globally will be almost as expensive as the legacy MPLS networks.

2. Include all disciplines of IT in the program kickoff.

The new direct-to-internet architecture will touch network, security, endpoint, server, and application teams. Include each team from the beginning with a clear end-state goal. This will help alleviate the political problems that pop up in transformation programs when the goals of each IT discipline are not communicated across the various leadership team. Everyone has to understand “what is in it for me.”

3. Build a reinvestment model with finance.

- Organizations will most likely recognize savings as they start to move to a cloud-enabled network architecture and move their data center workloads. Build a model with finance teams to reinvest a portion of the savings into technology that focuses on improving end-user experience.
- Find technology solutions that can monitor the experience of end users regardless of where they are located and send alerts when specific thresholds are met. This allows IT to focus on building proactive support processes as opposed to waiting for end users to complain about performance issues.

Successful transformation is often led by senior IT leaders

Leadership should empower employees to take risks and encourage them to challenge the status quo. Look at network, security, application, and identity architectures differently. CxOs need to convey their goals in terms of end-user experience, SaaS/IaaS adoption, enhanced security, and cost savings to all of IT. IT teams need to understand the overall context of the architecture they are tasked with building, as just replacing legacy point products will no longer work towards the goals of the CxOs.

CxOs must build the case for transformation with their business stakeholders on improved end-user experience (consistent access to applications regardless of location, which can in turn drive mobile workforce programs), enhanced security

(the threats are not going away, they are multiplying), and cost savings (most organizations are not "IT-focused" and their efforts should be focused on supporting their business, not managing email servers).

Multiple disciplines of IT with a collective mindset for change

The transformation programs will cover all of IT. CxOs need to sponsor the programs and make sure representation from each group participates in steering committees.

Overcome the political challenges associated with changing legacy architectures that have worked for 30+ years. The new architectures that support a cloud-enabled enterprise are very foreign to people who have been supporting legacy network, security, data center, and application infrastructure. CxOs need to focus on the paradigm shift of service ownership. The capabilities to support this architecture will no longer be delivered by point products sitting in a data center managed locally, but the skill set from the teams will still be required. CxOs will still need people with network, security, and application skill sets in the cloud-first world, in addition to a progressive mindset. Their teams will have to learn that they deliver the capabilities to their business stakeholders in a different way. ”

Ready to transform your company?

Create business value with Zscaler today.

CONTACT US

REQUEST DEMO

https://www.zscaler.com/company/contact

https://www.zscaler.com/custom-product-demo

About Zscaler Zscaler was founded in 2008 on a simple but powerful concept: as applications move to the cloud, security needs to move there as well. Today, we are helping thousands of global organizations transform into cloud-enabled operations.