CATO
NETWORKS

The 4 Pains of Digital Transformation and How to Cure Them

What's Your Pain?

Like many enterprises, yours is in the throes of "going digital." Business executives look to digital transformation to improve profit margins, reduce costs, and deliver new customer experiences. But what does digital transformation mean for network infrastructure?

After consulting with hundreds of companies around the globe, we've found that "digital transformation" generally translates into four projects for CIOs and their teams:

Mergers and Acquisitions

Global Expansion

Rapid Deployments

Cloud Migration

All four projects add challenge and complexity—AKA pain—to the IT experience.

Those pains in large part relate to complexities introduced by legacy IT infrastructure. To understand why and how you can prepare your organization, let's look at each project, the pains involved, strategies needed to address them, and how the shift to a cloud-native, converged networking and security service — the Secure Access Service Edge (SASE) — can help.

The Four Pains

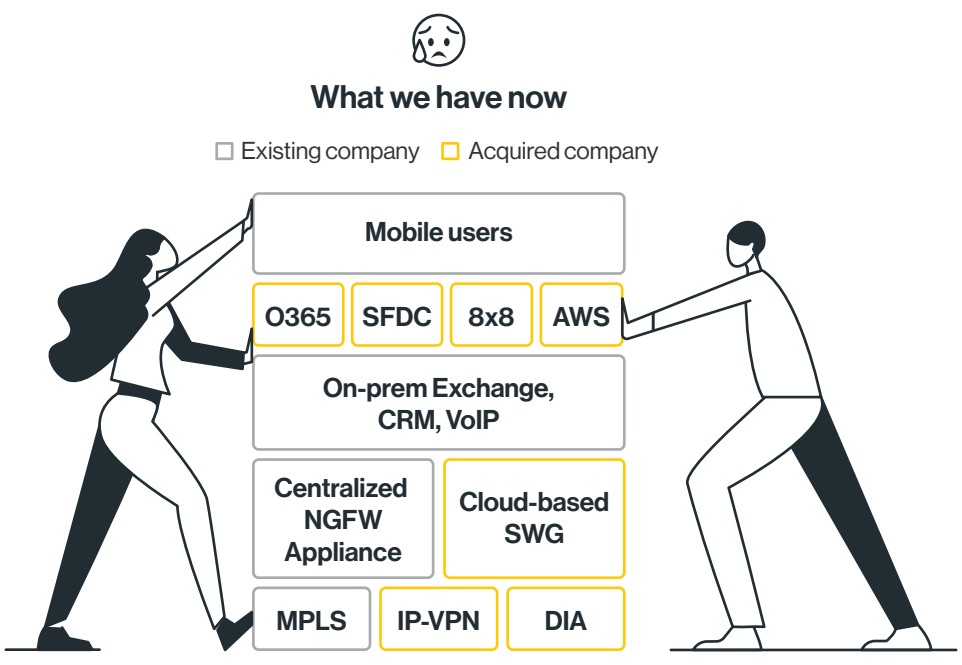
Mergers and Acquisitions (M&As)

When the CEO announces the organization's intent to acquire its largest competitor within two months, success of the merger and acquisition (M&A) business-wide project will rest on IT's shoulders. The speed at which an IT team can interconnect and rationalize everything from the network communications to security to the applications powering the company will determine speed of which the joint business can get operating and the overall success of the M&A.

The Scenario

In this example, the acquiring company has a legacy IT and WAN architecture that connects its multiple locations via MPLS. Internet and cloud access are provided via a centralized gateway, a NGFW appliance, in the corporate datacenter. Internal communications rely on Microsoft Exchange, CRM, and VoIP application servers, with some infrastructure housed in AWS.

By contrast the acquired organization is much more cloud and mobile centric, using Office 365, Salesforce CRM, and a Fuze, RingCentral or 8X8 for unified communications as a service (UCaaS). Security is provided by a cloud-based Secure Web Gateway (SWG). Offices have direct Internet access; Internet-based VPNs connect them to one another and to the cloud.



During this M&A, the IT teams needs to merge a legacy network with a cloud-centric one.

The IT Challenge

In just a few months, IT teams need to map existing and acquired networks, connect and integrate them, and get the integrated network up and running securely without major business disruption. To meet this broader IT challenge, CIOs must address infrastructure challenges across the IT stack:

Remote Access

Even before COVID-19, IT needed to equip users with remote access. With only one company heavily relying on mobile access, the IT team will likely look to adopt the legacy mobile solution companywide. Compelling reasons, such as performance, usability, and cost, may push the team to shift to a completely new mobile strategy. One way or another, IT will need to deliver a remote access solution for the complete enterprise.

Applications

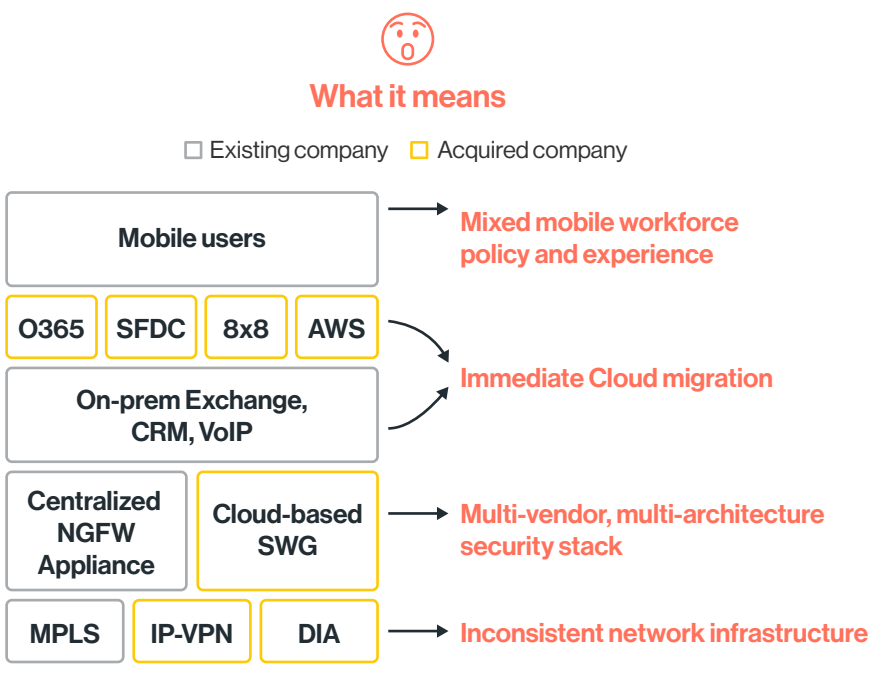
IT will need to rationalize the eMail, CRM, and VoIP deployments that exist on-premises and in the cloud. Given that half the applications reside in the cloud and organizations are moving to the cloud anyway, they will likely take the opportunity to move to the cloud. This will require an immediate cloud-migration project that alone could normally take several months.

Security

IT needs to impose a common security policy across the network. This ensures there are no holes for attackers to work around and that users can only access necessary, approved resources. The multi-vendor and multi-architecture security stack complicates this process significantly.

Network

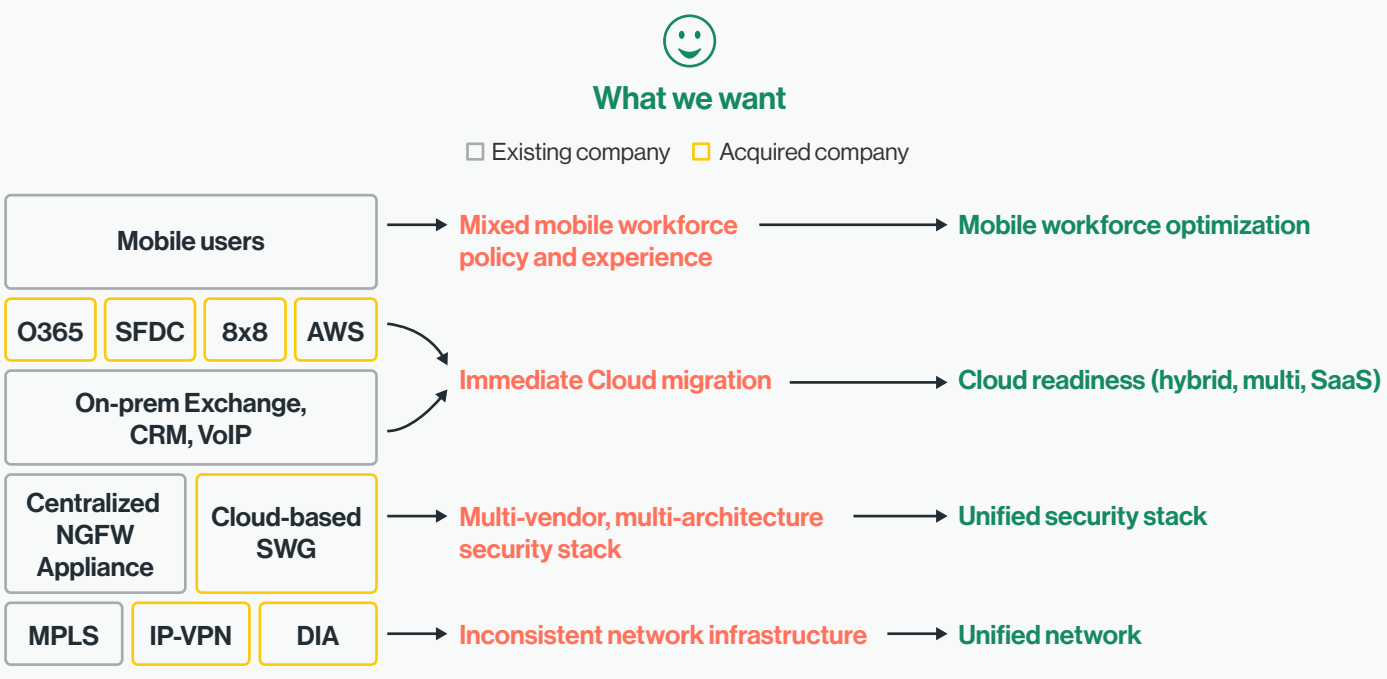
There isn't any one network now serving the complete business, which will complicate everything — accessing resources, managing the network, and more.



Merging the two networks results in pains across the IT stack

The Goal

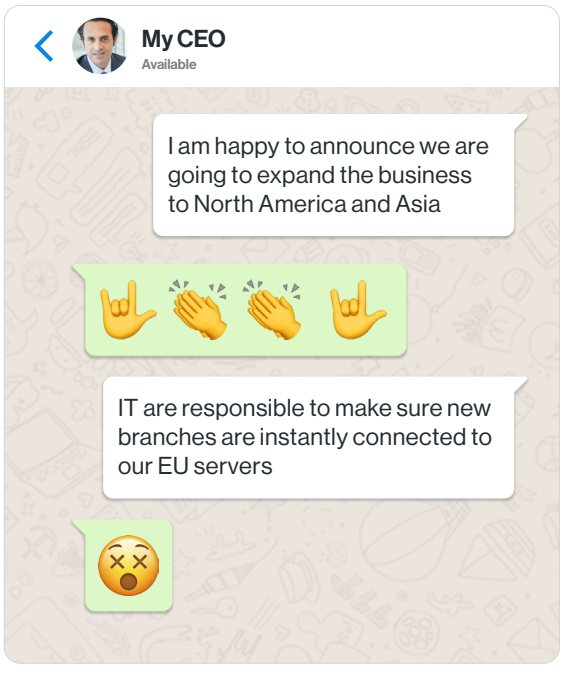
To address these challenges, IT needs to create a single unified network architecture across the merged organizations with a single management interface, unified security, and optimized mobile workforce architecture. The merged company should also undertake a cloud readiness assessment to determine the best, quickest strategy for cloud migration, including infrastructure, networking, security, and IT resource requirements.



To understand the tactics for implementing that strategy, **jump to The Solution below.**

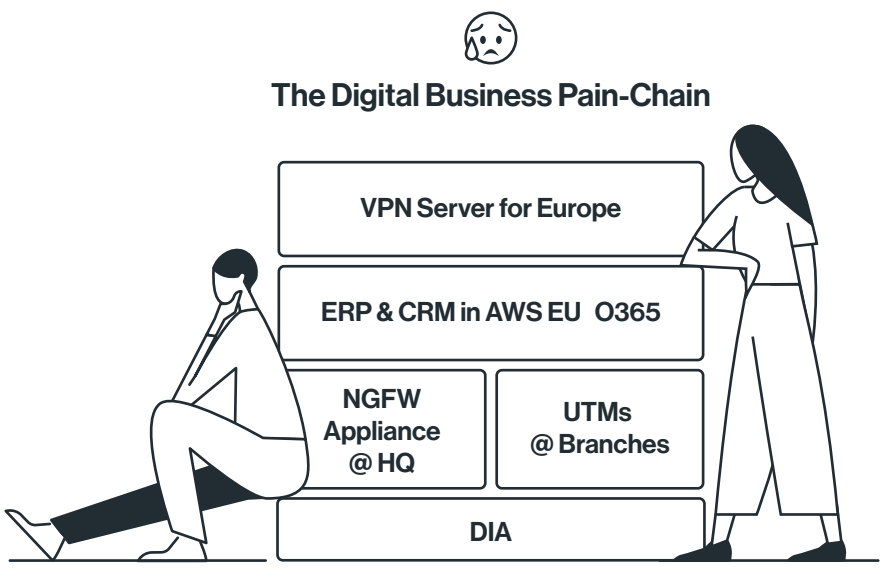
Global Expansion

The CEO intends to expand the company globally and turns to IT to make it happen. As any IT leader knows, growing into a remote region comes with many challenges. Encumbered by the latency of the increased distance, applications that performed so well in region will suddenly become sluggish. Additional security and network infrastructure will be required and must in turn be integrated with the company's existing infrastructure. In short, all aspects of IT management will be impacted by the increased distance, new infrastructure, and change in corporate cultures endemic to global expansions. Here's how to address them.



The Scenario

In this example, the company CEO announces a business expansion across North America, Europe, and Asia. The enterprise currently relies on a mobile VPN server at one of its European locations for connecting, securing, and managing remote and mobile users. Its corporate ERP and CRM applications run in an EU-based AWS datacenter. Office applications and messaging are provided by Office 365. Network security comes from a datacenter NGFW and UTM solutions deployed at several branch locations. The network communications at each location are provided through dedicated Internet access (DIA).



During global expansion, the IT team needs to open offices in new regions without compromising on security or performance

The IT Challenge

The IT team needs to provide consistent application performance and security across the entire globally dispersed organization, including in regions where the quality of network technology and services offered in the EU or North America is either unavailable or too expensive. To meet this broader IT challenge, CIOs must address infrastructure challenges across the IT stack:

Remote Access

Performance issues will have an impact on remote and mobile users in the new regions. They will also need ways to connect locally into the enterprise network to avoid the latency of connecting back to the European VPN server (see Application).

Applications

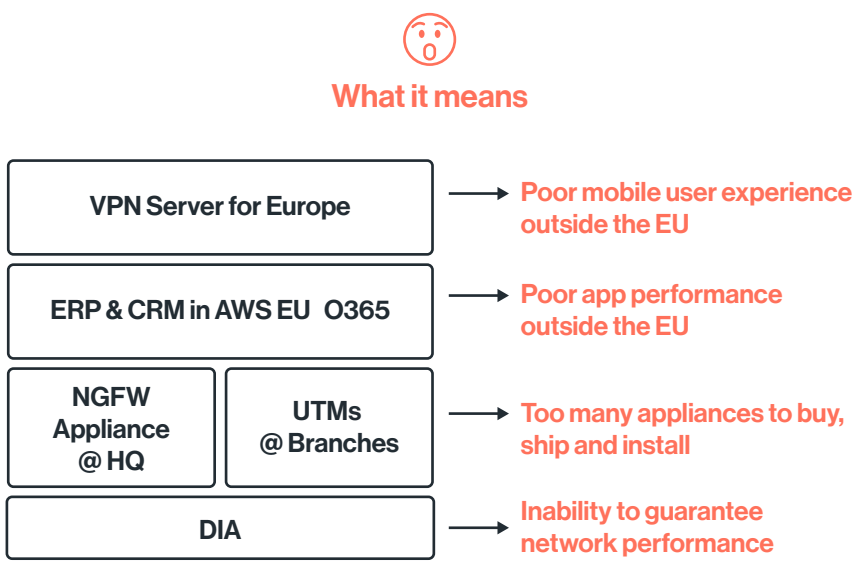
Since the data stores and applications are in the EU, US-based offices will need to send traffic back to the EU, adding latency that will disrupt the application performance.

Security

Since current security relies on firewall appliances, new appliances will need to be purchased, shipped, installed, and managed. This will take time and resources.

Network

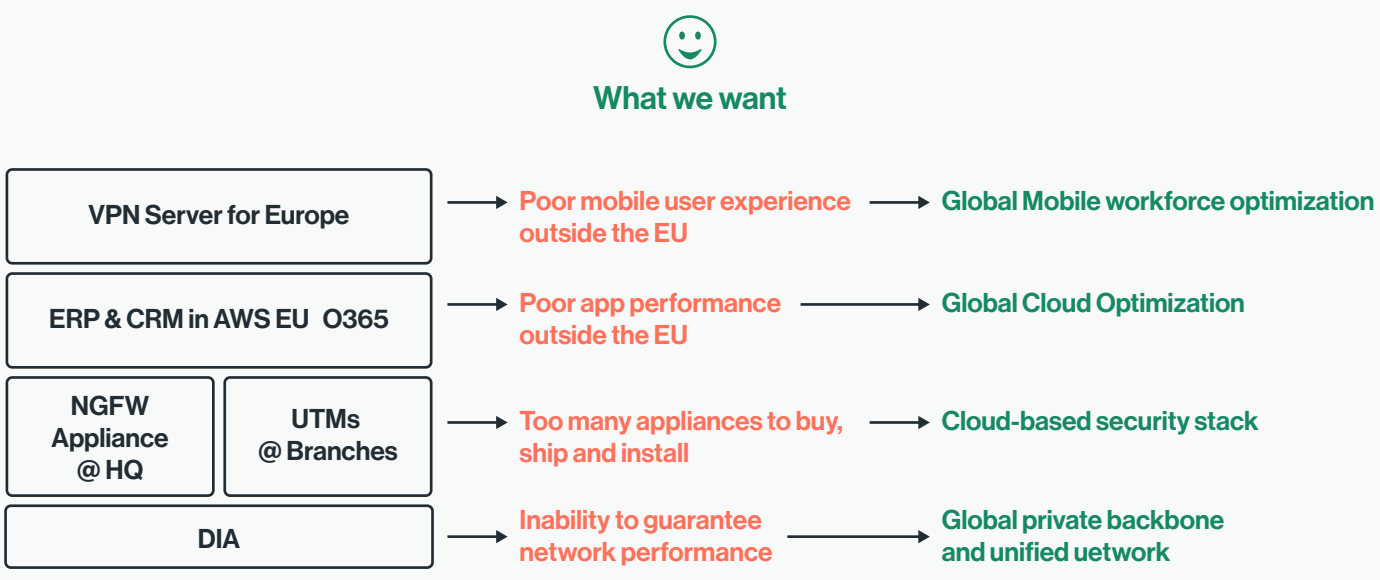
As office locations are deployed beyond the European Union, the enterprise will likely face declining application performance and a poor mobile user experience, due to the unpredictability and the higher latency of trans-Atlantic, Internet links.



Operational and network engineering challenges abound as users in the new region need secure access back to the EU.

The Goal

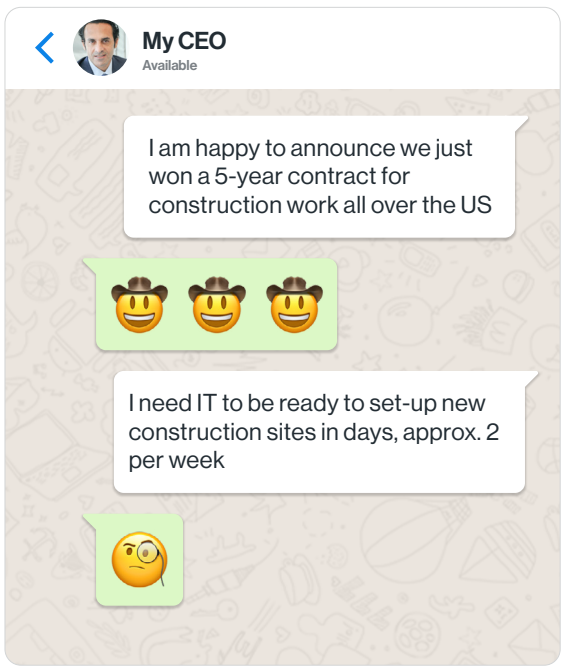
Ideally, the organization's IT globalization strategy should be built around a single, global optimized network architecture that connects branch offices and mobile users. Security should be provided everywhere via one global platform. Cloud application and cloud datacenter traffic should be optimized as well. Mobile users should be able to connect to this global network locally, avoiding the performance problems of first connecting back to the VPN server in the EU.



To understand the tactics for implementing that strategy, **jump to The Solution below**.

Rapid Deployments

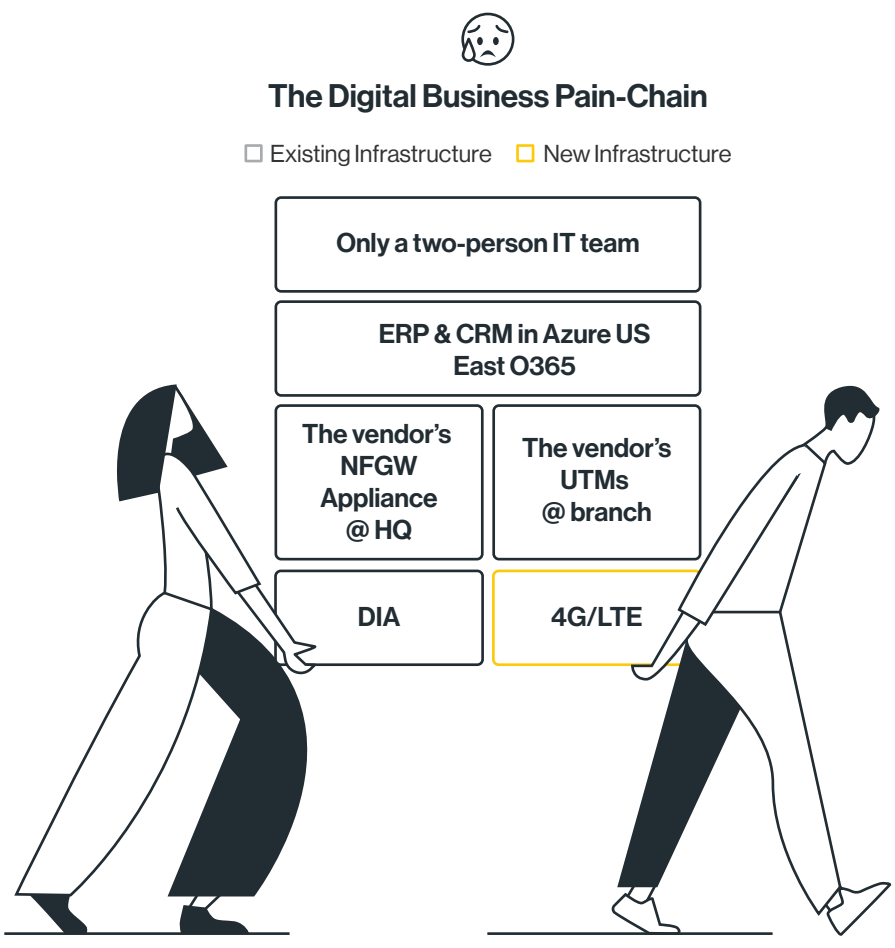
Whether you're in the construction or engineering industries that might only have hours and days to get teams on site or simply needs to open new offices in under a week, accommodating rapid business change easily is critical. In those cases, IT needs to get teams up and running with secure access to corporate applications and the Internet far faster than the weeks and months needed to open new offices with legacy enterprise deployments. How do you accommodate that kind of change? Let's find out.



The Scenario

In this case, the CEO announces a major new contract that requires setting-up scores of new sites across the U.S. at the rate of approximately two per week. Currently, the IT organization is lean with only a two-person IT team, so staffing and resources are an issue.

The company runs ERP and CRM applications in an eastern U.S. Azure datacenter and Office 365 for typical office applications and unified messaging. For security, it relies on a NGFW appliance in the corporate datacenter and the same vendor's UTMs at several locations. Site-to-site and Internet connectivity are currently provided by direct Internet access, but with the need to spin up sites quickly, the company will need to add 4G/LTE access at each of the new sites until the local telco can deploy broadband or fiber.



Rapid deployments bring numerous logistical challenges especially for lean IT teams.

The IT Challenge

Even if office space has already been acquired and the necessary last-mile connectivity is in place, opening two new sites every week still involves significant challenges:

Management

The biggest challenge is the lack of IT staff to execute a project of this magnitude while keeping the lights in the organization.

Applications

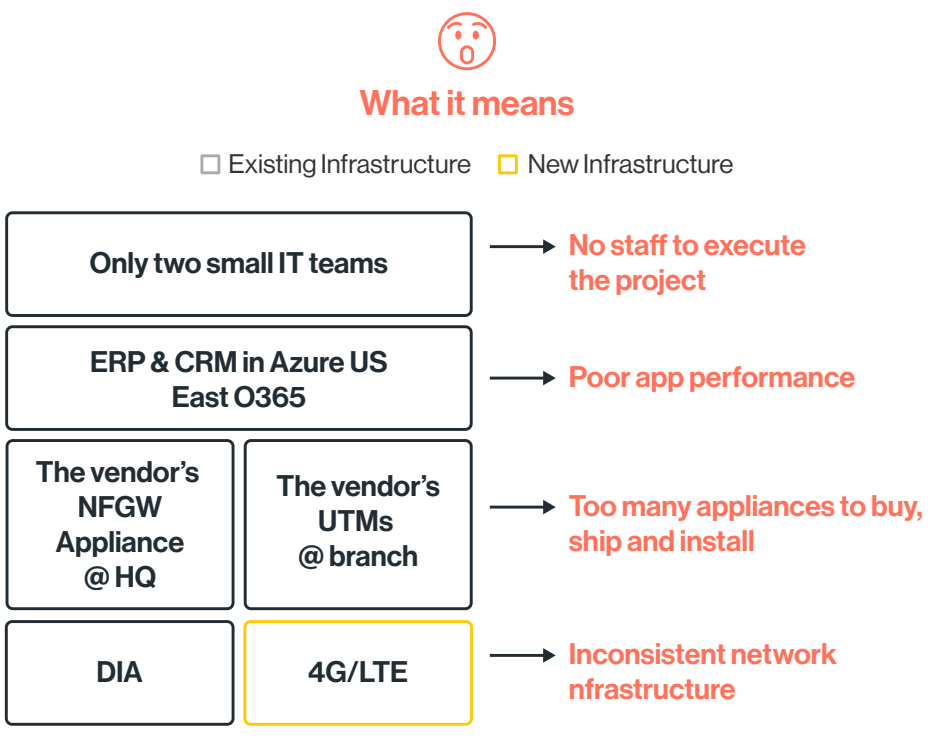
The application user experience will likely suffer as traffic is backhauled to the cloud datacenters in Europe.

Security

The IT team will be burdened with the significant logistics of purchasing, testing, and deploying the security appliances in each new location within such a short timeframe.

Network

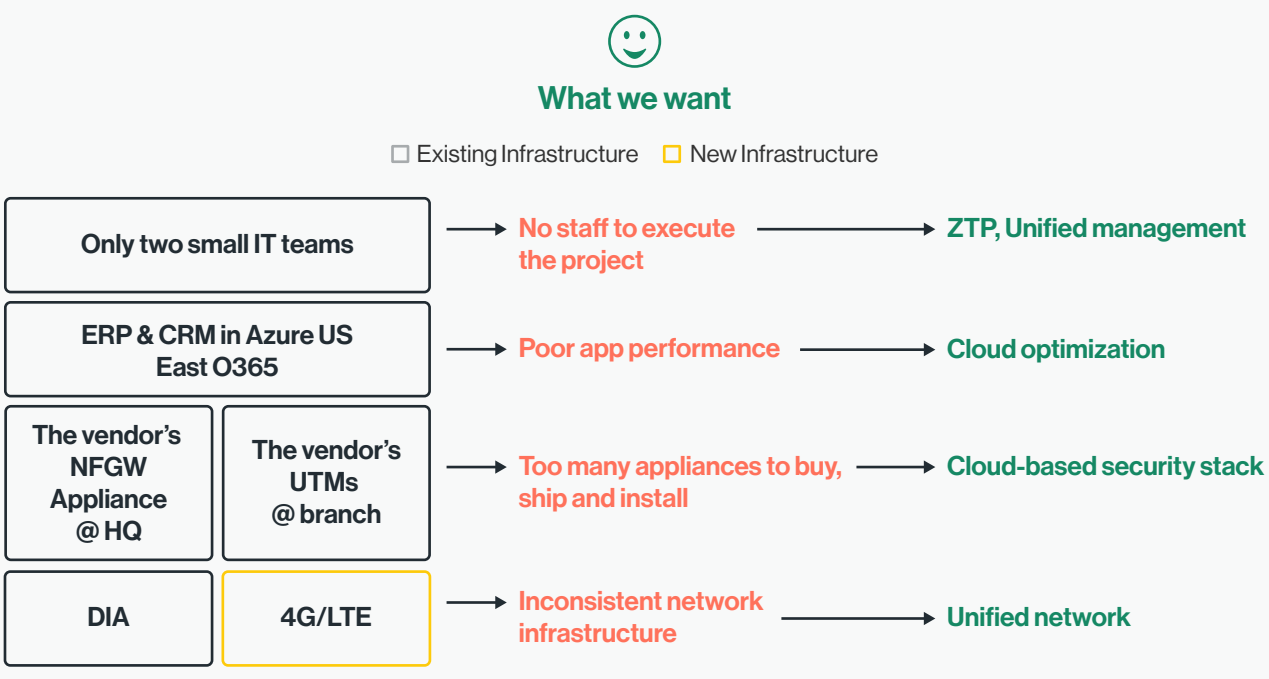
IT faces an inconsistent network infrastructure, with some sites on DIA circuits and new locations on 4G/LTE transitioning to DIA when available.



The Goal

With so many sites to deploy and so few IT staff, technologies that enable rapid site deployment (such as zero-touch provisioning) and simplified management are critical. Ideally, IT staff should be able to ship a preconfigured device that non-technical, on-site personnel can simply plug in and get up running quickly. Remote testing will be necessary as often zero-touch provisioning methods may not function behind local DHCP system.

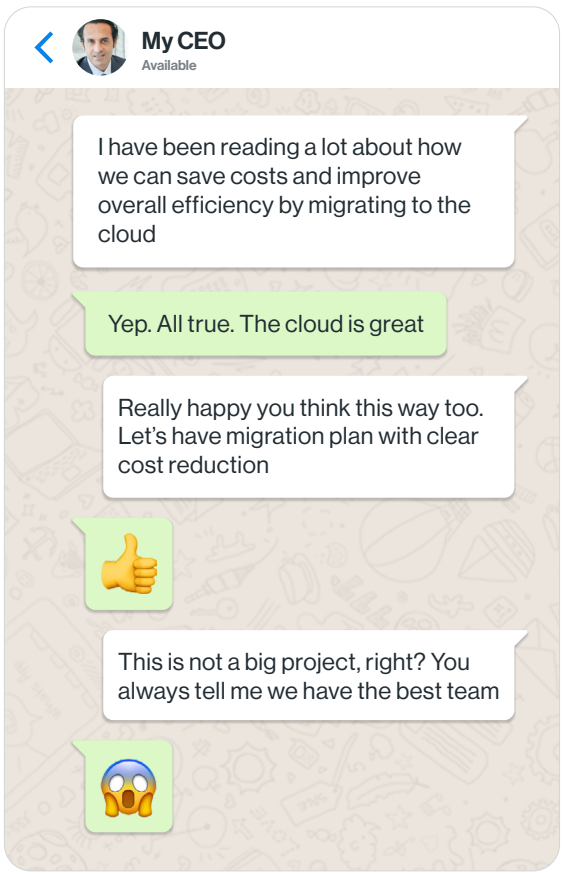
Site deployments need to include a cloud optimization strategy to protect the cloud experience. Getting security deployed quickly will be challenging with appliances. Firewall as a service (FWaaS) or a cloud-based security solution would be better solutions. Finally, having a single, unified network architecture across all sites will help simplify deployment.



To understand the tactics for implementing that strategy, **jump to The Solution below**.

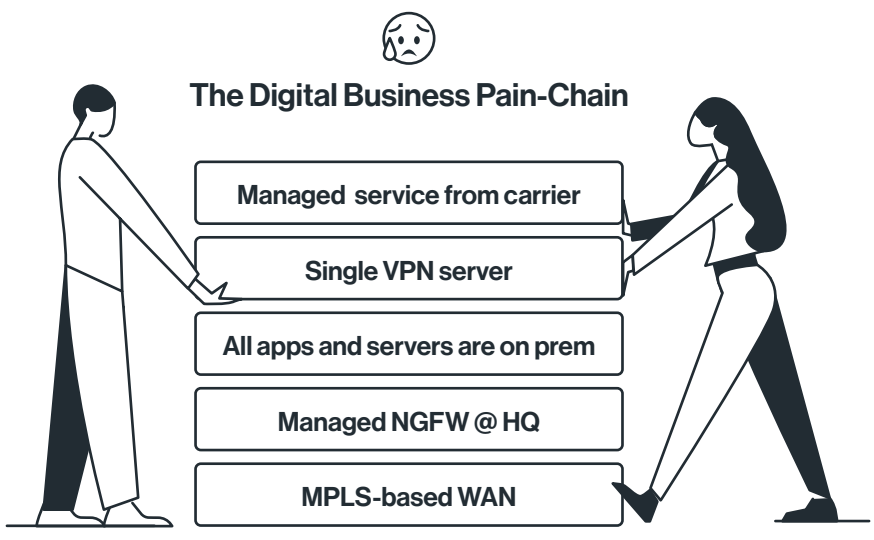
Cloud Migration

All companies have some cloud presence, even if it's just a few users running SaaS applications. And the benefits of the cloud are well known — easy adoption, rapid deployment and configuration, low maintenance, and, often, far less expensive than deploying the application yourself. So, what happens when the CEO decides to build on those benefits and insists that IT develops a plan to enter or significantly expand the company's cloud footprint? Alone this might be challenging. Cloud adoption and migration touch many teams within the IT organization. The cloud is particularly challenging for the infrastructure team when the global enterprise network is still based around legacy MPLS infrastructure. We'll detail those reasons why below.
Let's take a look.



The Scenario

The organization uses a managed, global MPLS service to connect branch offices to the company's datacenter. A NGFW appliance at headquarters acts as the secure Internet portal for the company. The network is fully managed by the MPLS provider. All current enterprise applications run in corporate datacenters. Remote and mobile users connect back to a VPN server.



With cloud migration, the IT team overcome the limitations of legacy MPLS architectures.

The IT Challenge

Developing a comprehensive cloud migration plan must account for not only cloud-specific costs but also the processes and technologies needed to migrate and support the cloud:

Management

Changes will take ages and cost a fortune as the MPLS provider becomes the gateway to everything.

Remote Access

Backhauling remote access traffic to a single VPN server before accessing the cloud will lead to a poor home and mobile user experience.

Application

One thing IT leaders know is when you make a radical change, such as moving applications to the cloud, there is a significant learning curve involved. There are bound to be issues, whether in the application domain or in the network domain. But the legacy organization lacks a cloud practice, making the transition particularly painful.

Security

Having a single NFGW at the headquarters means no control and no branch office security.

Network

The capacity and architecture of the underlying MPLS network are not sufficient for a cloud migration. Bandwidth upgrades and other architectural changes will need to be budgeted for in the cloud migration project.

What it means

Managed service from carrier	→ Changes will take ages, cost a fortune
Single VPN server	→ Poor mobile user experience
All apps and servers are on prem	→ No cloud practice. Potential crisis
Managed NGFW @ HQ	→ No control, no branch office security
MPLS-based WAN	→ Capacity and architecture doesn't fit

The Goal

Rather than staying with an aging MPLS architecture that is unsuited for the cloud, the organization should find a solution provider that can offer a high-capacity, Internet-based WAN and cloud-based security and mobile access solutions.

Such a solution will reduce the costs and delays of working with the telcos while providing a network with the capacity and architecture to support cloud migration. It will also ease cloud access, particularly if it includes a global, private backbone. With an FWaaS or cloud-based security platform, the IT team will be able to make security policy changes faster. Cloud-based mobile access will eliminate backhaul that undermines remote performance.

What we want

Managed service from carrier	Changes will take ages, cost a fortune	Self-service, simplicity, great support
Single VPN server	Poor mobile user experience	Cloud-based mobile access
All apps and servers are on prem	No cloud practice. Potential crisis	Easy cloud access and optimization
Managed NGFW @ HQ	No control, no branch office security	Unified cloud-based security
MPLS-based WAN	Capacity and architecture doesn't fit	High-capacity Internet-based WAN

To understand the tactics for implementing that strategy, **jump to The Solution below**.

The Solution

Each of the use cases described above has its unique challenges, but there are five major pain points common to all of them.

Network limitations

Current IT networking solutions are too varied and complex, with no unified management and no single private backbone.

Security limitations

Multiple security solutions yield inconsistent protection and become increasingly difficult to manage.

Cloud limitations

Connecting everyone to cloud datacenters and applications with current IT architectures is often challenging and complex, and yields little visibility and control over cloud applications.

Mobile limitations

Current mobility solutions deliver poor mobile scalability, performance, and security.

Management limitations

The current multi-vendor management architecture yields limited visibility and performance with maximum complexity. With carrier solutions, the main issue is usually loss of IT control.

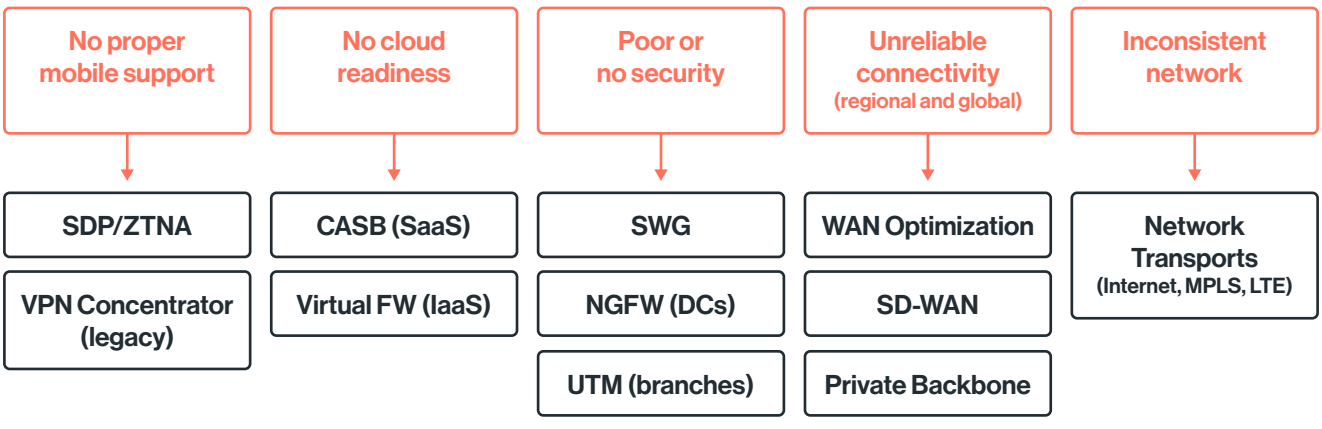
Solving Those Pains with Appliances: What's It Like?

Solving these five pains and challenges can take two possible routes. The first, as we've alluded to, consists of buying lots of appliance and software solutions for WAN connectivity, location security, and mobility—including SD-WAN appliances and next generation firewalls—and deploying them to multiple sites.

Unfortunately, for M&A, global expansion, rapid deployments and large cloud migrations, the appliance or software strategy can quickly get complex and overwhelming. Organizations often find themselves spending too much time and too many staff resources researching and acquiring scores of solutions from different vendors and struggling with all the different installation challenges and management interfaces they present. Maintaining and updating appliances requires experienced staff. Support across multiple vendors can be frustrating as each blames the other for the inevitable glitches and headaches that come up.

Integrating solutions from different vendors can also be challenging, sometimes even impossible, resulting in siloed network and security architectures that leave gaping holes in the security fabric. Monitoring and mastering so many different management interfaces is time consuming and yields limited, fragmented visibility.

Finally, appliances have limited scalability, which can lead to performance issues and frequent upgrades, adding even more expense and waste of IT time and resources.



From Pain to Products: The Many Technologies Needed to Meet Today's IT Challenges

Instead, Solve Those Pains with SASE

There is an alternative solution, however, that eliminates most of the challenges and headaches of appliances, while providing better, more consistent enterprise network wide network performance and security. SASE represents an IT architectural transformation that merges WAN connectivity and security for all enterprise locations and mobile users into a single global cloud service.

As defined by Gartner, SASE convergence networking and security into a single platform that is:

Cloud native

All networking and security functions are implemented in the cloud, where SASE leverages key cloud capabilities such as elasticity, adaptability, self-healing, self-maintenance, and global reach. Like other cloud solutions, SASE slashes upfront costs and delivers low monthly expenses and total cost of ownership, as maintenance, updates and management are mostly handled by the SASE provider.

Edge independent

Edge independent: SASE creates one network for all company resources, including company and cloud datacenters, branch offices, and mobile users.

Globally distributed

Globally distributed: With SASE, full networking and security capabilities are available everywhere on earth and deliver the best possible experience to all edges.

Identity driven

User identity--not IP address--determine the network experience, including QOS, route selection, security policies, and controls applied. This approach reduces operational overhead by enabling companies to develop one set of networking and security policies for users, regardless of device or location

SASE addresses the five pain points of digital transformation.

Management

SASE provides a single management interface for all networks, security functions, locations, and mobile users, transforming complexity and loss of IT control into simplicity and total control. Many SASE solutions enable user self-service, so new locations and mobile users can be added and configured quickly and easily.

Mobile

Mobile users connect to the same fast, cloud-based network as all other locations and resources, so there is no difference in performance, scalability, security, or productivity. Mobile users get the same work experience and productivity they get at the office. IT can add hundreds of new mobile users without any performance, security, or resource issues.

Application

SASE connects cloud datacenters to the same global network as other corporate locations and mobile users and manages those connections with the same management interface. Cloud connections are already preconfigured, so connecting to any SASE-connected cloud service is quick and simple.

Security

SASE provides all locations and users with a single, comprehensive, cloud-based enterprise security stack, including a NGFW, anti-malware, CASB, SWG, ZTNA/SDP, and IPS all managed under a single console.

Network

SASE connects every global location and mobile user to a single high-performance cloud-based network with a single management interface.

Cato: The SASE Platform of Today — And Tomorrow

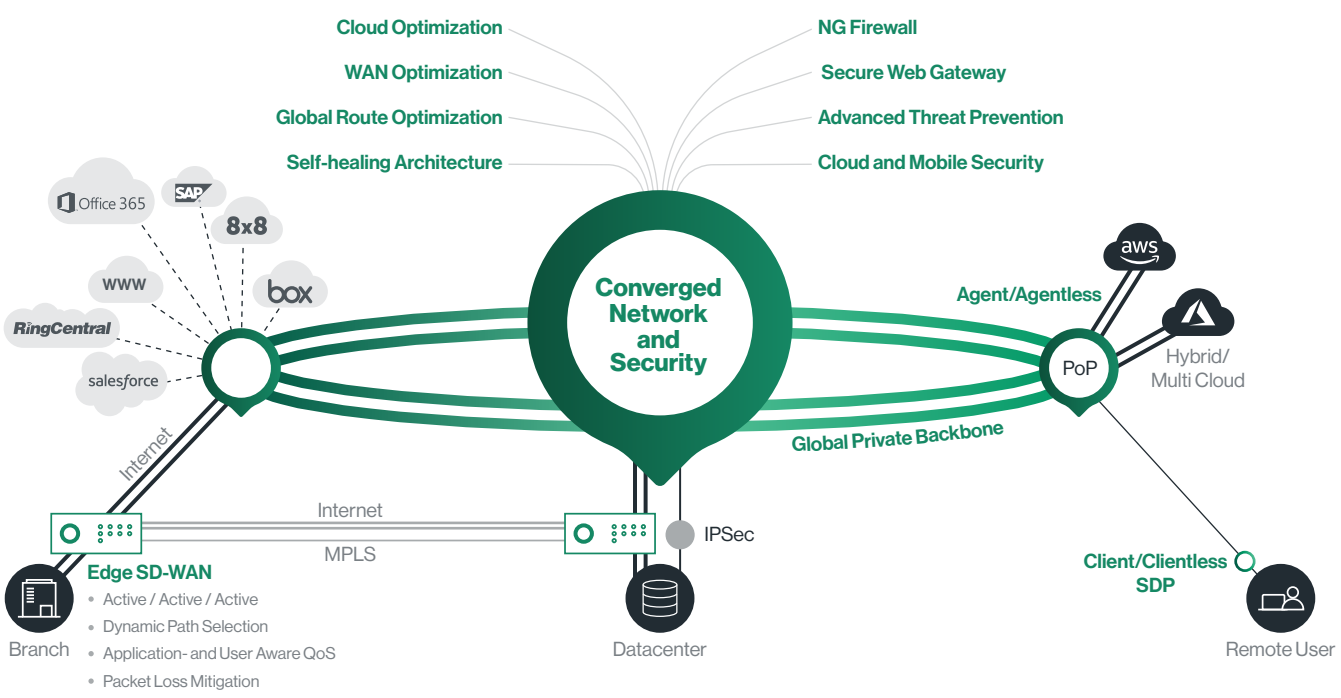
Cato is the world's first SASE platform, converging SD-WAN and network security into a global, cloud-native service. Cato optimizes and secures application access for all users and locations, including branch offices, mobile users, and cloud datacenters, and allows enterprises to manage all of them with a single management console with comprehensive network visibility. Cato's SASE platform has all the advantages of cloud-native architectures, including infinite scalability, elasticity, global reach and low total cost of ownership.

Connecting locations to the Cato cloud is as simple as plugging in a preconfigured Cato socket appliance, which connects to the nearest of Cato's more than 60 globally dispersed points of presence (PoPs). Mobile users connect to the same PoPs from any mobile device via a simple piece of software that is easy to install and use. With Cato, new locations or users can be up and running in hours or even minutes, rather than days or weeks.

At the local PoP, Cato provides an onramp to its high-performance global private backbone and security services. Cato monitors traffic and selects the optimum path for each packet across the backbone for performance that is as good or better than legacy MPLS. Since mobile users run across the same backbone as all other resources, the remote access experience is no different from working at the office.

With Cato, customers can easily migrate from MPLS to SD-WAN, optimize global connectivity to on-premises and cloud applications, enable secure branch office Internet access everywhere, and seamlessly integrate cloud datacenters and mobile users into a high-speed network with a zero trust architecture.

Whether its mergers and acquisitions, global expansion, rapid deployments, or cloud migration, with Cato, the network and your business are ready for whatever is next in your digital transformation journey.



Cato. The Network for Whatever's Next.

Cato Cloud

Global Private Backbone

Edge SD-WAN

Security as a Service

Cloud Datacenter Integration

Cloud Application Acceleration

Mobile Access Optimization

Cato Management Application

Managed Services

Managed Threat Detection and Response (MDR)

Intelligent Last-Mile Management

Hands-Free Management

Site Deployment

ISO 27001 Certified

GDPR Compliant