

Rebuilding the enterprise
in the age of cloud



REBUILDING THE ENTERPRISE IN THE AGE OF CLOUD

Cloud services are integral to an enterprise's application strategy as more businesses move their workloads away from traditional on-premise environments. As cloud adoption grows across Europe and around the world, so too do expectations as enterprises increasingly require secure, high-performance and cost-effective access to public clouds, such as Microsoft Azure, AWS, Google Cloud Platform and a multitude of SaaS providers.



In the midst of this upheaval, enterprises want the best of both worlds. They want to protect and retain control of their most sensitive data, meet compliance requirements and maintain application performance – which means low latency, predictable routes into the public cloud. On the other hand, as IT budgets continue to shrink and expert resources are scarce, public Internet connectivity can appear to be an attractive option, but remains at best a partial solution.

Over the last five years enterprises have tried various approaches to bridge the gap. The most successful has been moving the enterprise edge to neutral colocation data centre facilities, while migrating applications out of on-premise to a mix of those facilities and the cloud. This approach offers high performing, secure connections to public cloud and SaaS services that will support business transformation, while enabling enterprises to centralise the management of their network and application environment and keep data on private, managed infrastructure where required.





Embracing a new network architecture

Organisations are having to manage very complex environments that comprise legacy and new cloud-native applications, plus in-house and outsourced IT – a situation that will not change for at least the next ten years. Enterprises, service providers and systems integrators increasingly want to connect to multiple cloud based services, but have found that the challenges of variable and opaque internet performance, the difficulties of service orchestration across such a wide range of services, and an ever-broadening security perimeter demand another approach.

In the early days of this revolution, connecting to the cloud via the public Internet was driven by frustrated users signing up for services outside the control of corporate IT – cue a boom of articles a few years ago warning us about the dangers of “shadow IT” and “consumerisation of IT.” Since then, many of these services have become integral to the corporate IT infrastructure and have been largely reined in and embraced by IT departments to reduce the risk of security and regulatory breaches. However, we have found that the enterprise network architecture has often not evolved to reflect the critical nature of the services these applications provide. We have seen that today, enterprises have on average between three and five IaaS/PaaS providers with managed IT connectivity, but 15-20 SaaS providers. Our experience of the Internet at home is generally one of reliability and good performance for the services we require, such as Skype video calls, enjoying Netflix in 4K, gaming and online banking.

However, enterprises have often found that its purpose for mission critical services is a different beast altogether, particularly when applications are split between on-premise/neutral colocation and the cloud. Latency decreases cluster performance by an inverse square law, to the point that even small latency variances have a disproportionate effect on application experience, and volumes of traffic are growing beyond volumes suitable to an ISP. In the worst case scenario, the loss of connectivity – or poor latency or throughput – can cause data to get out of sync and create a “split brain” problem where the data gets out of sync, resulting in two versions and causing an immensely costly and time-consuming reconciliation exercise. We have found that the enterprise requires a much more dependable and secure connection than the Internet can predictably provide, and it’s starting to drive them towards private cloud connections.

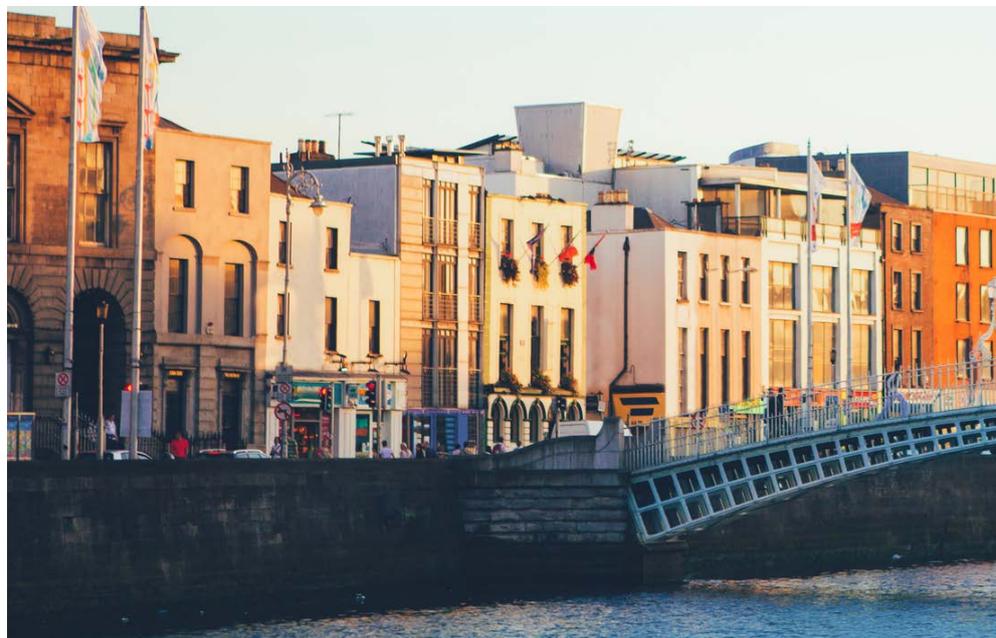


Today, enterprises have on average between **3 & 5** IaaS/PaaS providers with managed IT connectivity

...but

15-20

SaaS providers



Safe and secure

Five years ago, network security for cloud connectivity was somewhat of an afterthought, and any thought that was applied generally leaned towards IP Sec or SSL encryption being sufficient for the kinds of applications and workloads being run in the cloud. In 2020, the situation is quite different, with critical applications held entirely within the cloud and confidential company data and private information constantly shuttling between private and public environments. As such, the cloud environment needs to be treated as an integral part of the enterprise network environment, with all the auditability, visibility and manageability that implies. It's certainly the case that public Internet connections can be secured. Much more difficult is the visibility and management of the tunnels over the Internet, as the number of secured endpoints proliferate enterprises have found it's more complex and costlier than they anticipated. Security and performance therefore run hand-in-hand, as guaranteeing bandwidth and throughput for apps without the attendant security controls being in place is no longer acceptable.

The rise of the colocated enterprise edge

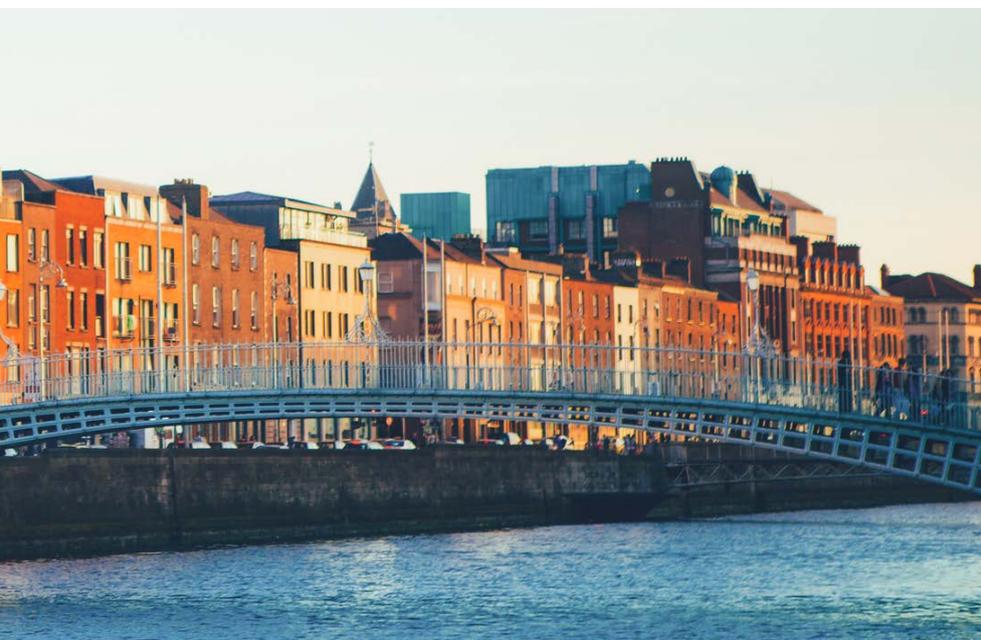
The growth story over the past five years has been the relocation of the key enterprise network edge functions in a neutral colocated facility. In parallel, adoption of hybrid cloud, where application workloads are split between private and public cloud and supported by the colocated enterprise edge, is rapidly accelerating. This approach is solving the performance concerns associated with the public Internet, putting enterprises just a few milliseconds away from the leading CSPs.

Many enterprises began taking space and power for enterprise edge services to start the integration of the cloud platforms into their environment. They then grew the space as they moved private and internal applications to colocated facilities, migrating to their new hybrid environment and shutting down legacy on-premise facilities.

In this design, it's not just the volume of connectivity that is enabled, it's also the quality and richness of traffic. Colocating in a data centre provides access to a host of connectivity providers and a highly competitive environment in which enterprises can renegotiate their contract with their existing carrier or provider, or easily find another partner that offers a more cost-effective alternative. In addition to boosting connectivity, colocation also reduces enterprises' costs and reduces the bandwidth required to manage their own data centres – or eliminates the need for them altogether.



The growth story over the past five years has been the relocation of the key enterprise network edge functions in a neutral colocated facility.



To see how this works in action, let's look at an example of one Interxion customer's journey over the past five years:

Our customer, a large enterprise, operated three private data centres and was using a carrier to provide a private IP network connecting over 50 main offices and 2000 branch locations across Europe. Needing to update their applications and reduce costs, they started a long-term program to close down the private data centres and reduce network costs. At the same time, they wanted access to a greater choice of IT service suppliers and a network that wasn't a pure "one size fits all" approach.

1. Deploy network points of presence

Their first step was to deploy network points of presence (PoPs) within four Interxion data centres in their four critical markets. This provided connectivity to a number of local and regional ISPs to improve local connectivity from and to their branch offices and for their remote employees, and defined the new enterprise network edge perimeter.

2. Direct access to AWS for DevOps

They also added two private connections to AWS for their dev/ops environment to support their cloud migrations.

3. Workload analysis

A multi-year "cloud first" programme began, starting workload migration by looking at the types of applications they had on their network, identifying which ones they wanted to continue to invest in and those they wanted to replace with SaaS alternatives.

They found a number of legacy applications or workloads that they had to keep, but decided to move them close to the public and private cloud to make their setup hybrid and, wherever possible, put data and applications in close proximity to each other.



4. Getting applications cloud-ready

Over time, a number of SaaS providers were identified, and integration work was undertaken in AWS.

5. Redeployment of edge network functions

Project stages have since included the redeployment of edge network functions, including network security, network performance management, and remote access aggregation, out of their own facilities and into the Interxion facilities. This has also greatly reduced the need for tromboning traffic in and out of their facilities.

6. Deploying the workload

The decision was also made to migrate to Office 365 and Skype for Business, so another two private connections were established into Microsoft. In particular for Skype, the customer found a significant improvement in call quality by moving to private connectivity, with a positive impact on the speed of internal take-up of the service.

7. Close down on-premise data center

Internal legacy applications have been almost entirely migrated into two main Interxion locations, colocated with the network PoPs and private connections to the cloud. While one private data centre has already been shut down, they expect the other two to be closed in 2020.

Results

1. Reduced direct costs by 90% through Direct Connect to the public cloud vs public internet.
2. Significant savings on network costs.
3. Lower internet costs through use of local connectivity providers.
4. Saved on IT costs by optimising their applications and killing off some legacy workloads.

Conclusion

By adopting this colocated hybrid approach, enterprises are increasing business agility and optimising their networking strategies by interconnecting networks, cloud platforms, customers and partner communities in one place. Colocating IT infrastructure alongside the cloud platforms of their choice has enabled enterprises to improve workload performance and ensure the best possible connectivity, with an SLA-backed 99.999% network uptime.

The Interxion Cloud Connect platform is present in all 13 Interxion regions and provides any-to-any connectivity between customers and CSPs. Enterprises, carriers and IT service providers that require connectivity to a specific cloud service provider or region are increasingly connecting into our pan-European network through either a single connection or dual connections for redundancy, with one customer running almost 50 cloud connections across the platform.

To meet growing cloud demands, enterprises must focus on network performance and proper distribution of workloads. More and more enterprise budget is being allocated towards supporting cloud services, but adequate consideration of the networks that get them there have proved to be a major determinant of the success of enterprise cloud strategy over the past five years. Accessing cloud-based applications through the public Internet simply hasn't delivered the level of performance required to make cloud transformation projects a success.

But now, using Interxion at the centre of a hybrid cloud strategy, enterprises can achieve secure cloud connectivity whilst housing their own private cloud infrastructure and network edge services in our highly secure data centres. This is supported by the added assurance of rapid provisioning, 99.999% uptime and 100% guaranteed throughput. The next five years will undoubtedly bring just as many changes as the past five, and we're looking forward to continuing to play a crucial role at the centre of the transformation of enterprise IT.



About Interxion

Interxion (NYSE: INXN) is a leading provider of carrier and cloud-neutral colocation data centre services in Europe, serving a wide range of customers through over 50 data centres in 11 European countries. Interxion's uniformly designed, energy efficient data centres offer customers extensive security and uptime for their mission-critical applications. With over 700 connectivity providers, 21 European Internet exchanges, and most leading cloud and digital media platforms across its footprint, Interxion has created connectivity, cloud, content and finance hubs that foster growing customer communities of interest. For more information, please visit www.interxion.com

Data Centre services across Europe



www.interxion.com
customer.services@interxion.com



International Headquarters
Main: + 44 207 375 7070
Email: hq.info@interxion.com

European Customer Service Centre (ECSC)
Toll free Europe: + 800 00 999 222 / Toll free US: 185 55 999 222
Email: customer.services@interxion.com

Cofounder: Uptime Institute EMEA chapter, **Founding member:** European Data Centre Association, **Patron:** European Internet Exchange Association, **Member:** The Green Grid, with role on Advisory Council and Technical Committee, **Contributor:** EC Joint Research Centre on Sustainability, **Member:** EuroCloud.

Interxion is compliant with the internationally recognised ISO/IEC 27001 certification for Information Security Management and ISO 22301 for Business Continuity Management across all our European operations.
© Copyright 2020 Interxion. BP-ENT-HQ-REBUILD-IE-eng-4/20