

Getting physical with Hybrid Cloud security

Interxion Cloud Connect service offers enterprises the most secure and resilient Hybrid Cloud solution.

In this follow-up paper we outline how Interxion Cloud Connect service offers enterprises the most secure and resilient Hybrid Cloud solution. Combining physical security, round the clock maintenance and support, and more than enough redundancy to cope with the unexpected, Interxion's colocation data centers help enterprises realise the true potential of Hybrid Cloud.



Executive summary

- Every business is a data business, and the cost of failing to secure that data, both logically and physically, can be devastating.
- On-premise data centers have served many organisations well to date, but are ill equipped for handling the demands of a 24/7, cloud-driven business world.
- For most businesses security isn't the core competency, and so the challenges of maintaining enterprise-grade physical security can leave in-house staff over-stretched and exposed to vulnerabilities.
- Interxion Cloud Connect service provides private, high performance and cost efficient interconnectivity for enterprises to their cloud providers of choice, including Microsoft ExpressRoute and AWS Direct Connect, bypassing the public Internet for their connection to the clouds.
- Utilising Cloud Connect as part of your Hybrid Cloud strategy, your data center operations can have the highest degree of physical security, supported by built-in redundancy to cope with even the most extreme situations.

Secure from the ground up

Senior business leaders know the impact a data breach could have on their business. Each year, corporations spend [more than \\$90 billion](#) globally on cybersecurity related software and services, seeking to prevent malicious attacks such as account hijacking, phishing and malware injections. If successful, any of these attacks could have a devastating effect on a business's operations, its relationship with customers and stakeholders, and its corporate reputation more broadly.

As more organisations embrace cloud services, connecting their on-premise data center to cloud gateways via public Internet, the need for logical solutions to secure data from cyber threats becomes more pressing. Yet, even with the latest and greatest logical security, your company data is only as secure as the physical environment and controls you have in place to prevent unauthorised access. Indeed, it's estimated that physical actions play a role in almost [one in ten](#) of all data breaches.

If malicious actors can gain physical access to cloud systems then even the most sophisticated cyber defence becomes redundant. Data plays an increasingly important role in the world of business, and so enterprises need to know that their data will remain secure whatever the circumstances. Companies must therefore create a secure physical environment for their data, supported by unfaltering access controls. It's for this reason that more and more businesses are now hosting applications and storing data in colocation data centers. These colocation facilities represent a favourable alternative to hosting data on-premise or in a dedicated data center, offering lower cost, greater reliability and 24/7 local support. As physical security becomes a greater organisational priority, colocation allows companies to safeguard business-critical data and hardware from loss, theft or damage.

In this paper we'll make the case for Hybrid Cloud, showing how Interxion's Cloud Connect offers customers safe and reliable access to cloud services. You'll learn what Cloud Connect is, how it functions, and how it can benefit your organisation in ensuring the highest level of physical security and resiliency for your data center operations. We'll also discuss how [Cloud Connect](#) can help your organisation to adapt quickly to abnormal or unpredictable circumstances without inhibiting or relegating the critical importance placed on security.

ABOUT CLOUD CONNECT

To maximise the benefits of next generation technology for their business, enterprises need the agility, scalability and cost-effectiveness of cloud services. Managing complex IT stacks that can comprise of legacy and cloud applications, in-house and outsourced IT, enterprises want the flexibility to benefit from a blend of services, delivery and deployment options. This makes Hybrid Cloud the natural solution to meet these needs.

However, with this opportunity comes restraints and there is little more constraining to innovation than the threat of insecurity. As part of a hybrid approach, businesses want to know how they can rely on the public cloud. However, there are significant barriers to accessing cloud services via open Internet connectivity: the need to protect sensitive data, meet compliance requirements, or safeguard application performance to name just a few.

The threat of data breach looms large over all organisations and industries. To embrace the true potential of Hybrid Cloud in a safe manner, enterprises need a cloud service delivery model that ensures access to business-critical data remains in the right hands.

For fast, reliable and secure cloud access, enterprises are finding private connect solutions offer the predictable performance their applications demand while bypassing the public Internet and its inherent security and performance flaws.

Introducing Cloud Connect

Cloud Connect is Interxion's cloud access service, which enables secure, private connections to multiple cloud providers from one physical connection in a carrier neutral data centres. With high-speed, secure connections to your cloud providers of choice, Cloud Connect provides a simple, fast and cost-effective way to create hybrid and multicloud IT environments and to move business-critical workloads and latency-sensitive applications to the public cloud. This allows your business to bypass the public Internet to avoid its inherent flaws, and rest assured that your data is connected straight into your clouds.

Cloud Connect is built with carrier-grade hardware offering a 99.999% service level guarantee, installed within a secured colocation facility and monitored 24 hours a day, 365 days a year. The service is available in 13 countries throughout Europe with Any-to-Any connectivity across Interxion's data center footprint.

Why Cloud Connect?

- Single physical connection to support multiple VLANs
- Order quickly and easily via our Customer Portal
- Secure, SLA-based Layer-2 Connectivity
- Speedy provisioning
- Any-to-Any connectivity across Interxion footprint
- Round-the-clock technical support

Cloud Service Providers

- Amazon Web Services
- City Cloud
- Google Cloud
- IBM Cloud
- Microsoft Azure
- Oracle Cloud Infrastructure

Interxion Data Centre Locations

- Amsterdam
- Brussels
- Copenhagen
- Dublin
- Dusseldorf
- Frankfurt
- London
- Madrid
- Marseille
- Paris
- Stockholm
- Vienna
- Zurich





KEEPING DATA PHYSICALLY SECURE

For most modern enterprises, data is one of the most precious assets. It's what distinguishes you from your competitors. It also embodies trust – your customers and other stakeholders have given you data on the promise that it will be kept secure and only used for defined purposes.

If you can't guarantee the physical integrity of that data and the applications that run it, then these relationships are at risk. It's with this purpose that Cloud Connect offers the most robust physical security possible.

The shortcomings of on-premise data centers

Conventionally, managing data on-premise made good sense. Having it in close proximity to your local network, and within arm's reach of your in-house IT team meant you had full visibility and control over your IT environment.

However, physical control over data doesn't equate to security. As the volume and velocity of data under an organisation's control continues to grow, and more businesses have a critical need to access cloud-based applications and services, the logic behind maintaining an on-premise data center starts to unravel.

Leaving aside the performance and security challenges of public Internet, on-premise IT is also vulnerable from a physical security perspective. The servers need to be maintained and monitored 24/7, access to the server room must be treated with strict authorisation, and logs of who's visited the premises must be kept for auditing purposes. This places a huge burden on in-house staff to be carrying out appropriate checks on a continual and consistent basis, and is also a time-consuming drain on valuable business resources.

For most organisations, this just isn't practical. Companies already face a big challenge in keeping day-to-day business running, and so security can easily be relegated in importance as more immediate priorities emerge.

Creating a secure environment

[Cloud Connect](#) addresses all of these flaws, offering robust physical security and top-grade access controls. As a rule, the more layers that a center can provide between the individual and your data servers, the greater the likelihood of reducing the risk of a physical breach.

Interxion data center buildings are typically designed with five layers of security, making them less susceptible to breach. These layers include the perimeter fence, the security gate and entrance, mantraps into the data centre, access systems into the rooms and secure, locked cabinets. Additional levels of security can be introduced such as lockable cages or containment aisles.

Moreover, the colocation facilities are staffed by security experts 24/7. It's their job to make sure your hardware is safe, so you and your staff have no need to worry. By entrusting your data center security to experts that are able to give unremitting focus to protecting your servers, you are able to unburden your staff and create a more sustainable cost structure around data center management.



Interxion five layer security concept

Trained security staff on-site 24x7

Complete data center building protected by a security fence

Multiple physical security layers including proximity cards, biometric access readers, CCTV, man traps

24x7 controlled access

ISO/IEC 27001 Information Security Management certified

The multi-layer physical security includes strong controls on admittance. No one is able to enter or leave Interxion facilities without proof of identity, all visitors are checked against customer-defined access lists and biometric readings are taken on an individual's first visit. Individualised access to rooms and cages ensures that the strict access is maintained throughout the facility. Further, all building areas are secured by CCTV and an alarm system, and a contracted, licensed security firm patrols the area, both inside and out.

With every potential vulnerability covered, housing even your most business-critical data in Interxion's data centers gives you the peace of mind that your data will be safe around the clock.





PREPARING FOR THE UNEXPECTED

It's not uncommon for enterprises to encounter unanticipated challenges in maintaining their data center operations. Maybe it's a power shortage, a surge in demand, or specialist staff being unexpectedly off work. In isolation, most organisations have the ability to cover small shortcomings without hindering security.

Where the problem is on a larger scale, or multiple unexpected events happen at once, the ability to reallocate resources becomes increasingly difficult. In extreme circumstances, such as an emergency situation or a natural disaster, it can put the physical security of an organisation's data center operations in jeopardy.

The risk of downtime

In such an instance, an on-premise data center – and the security protocols around it – could be severely compromised. Without access to normal systems, your in-house staff may be left blindsided as to which course of action to pursue. You may also find that the staff you have at your disposal on that particular day don't have the specific skills to deal with the issue, necessitating external support that may not be readily at-hand.

At the very least, the incident could cause a prolonged period of downtime that proves frustrating to staff and customers alike. At worst, the situation could leave you exposed to malicious actors, without the normal defences you'd have in place to prevent such a breach.

Ready for the unexpected

With Cloud Connect, however, strong contingency planning and resources are in place to maintain the integrity of operations, helping your organisation to maintain 'business as usual'.

In the event of disaster recovery, Interxion data centers have the most robust and redundant design possible. With inbuilt mechanisms to withstand even the most difficult situations, the facilities have more than sufficient redundancy to take a 'direct hit' to services and not see any downtime nor service loss in most cases. Equipment has its own cooling and redundant power to ensure continuous operation, and facility management can close off a customer's operations if there's any suspicion that they pose a threat to others.

Colocating from an Interxion data center also provides access to on-demand technical support, offering complete transparency and peace of mind to customers. This includes analysis report and calls on any issues even when not customer impacting. For any major issues, a call bridge with customers would be set up immediately, with subsequent updates at 15 minute or 30 minute intervals. The interconnection benefits of a colocation environment also means that you have MSPs in reach that can provide additional services to help maintain a secure IT environment.

CONCLUSION

Businesses need continuity. The costs of IT disruption can have a ripple effect across everything an enterprise does. When it comes to data, disruption through loss, theft or outage could have a profound impact that takes weeks or even months to recover from.

To keep data secure and resilient to unexpected challenges, you need a solution that's measured to your needs. Any gaps in oversight, maintenance and recovery can leave your whole business exposed, and provide a boon to those with malicious intent. It therefore makes good business sense to entrust data – from your routine workloads through to your business-critical applications – to those with the expertise to maintain its integrity, even in the most extreme circumstances.

[Cloud Connect](#) provides this capability. Moving your hardware to our colocation data centers means you can maintain private access to multiple clouds, safe in the knowledge that your physical server security maintained around the clock. With private interconnections to your cloud platforms of choice, you can ensure your data and applications are accessed only by those you've explicitly authorised and will remain operational if and when the unexpected occurs.

Regardless of your current level of cloud experience, using Cloud Connect lets you create a top-notch security environment around your cloud services. It reduces on-premise IT costs, limits exposure to the risks of public Internet-based cloud access, and provides access to the security expertise you need, whenever you need it. Cloud Connect also allows you to test the cloud in a low-cost, low-risk way. You are not tied into the service, and can tailor the setup and controls to your business needs, making sure you're secure from day one.

With everything taken care of, you can free up your internal resources to focus on what your business really needs – turning Hybrid Cloud into your competitive advantage.

If you'd like to learn more about [Cloud Connect](#) and how it can help you capitalise on today's Hybrid Cloud opportunity, download our Cloud Connect [product factsheet](#) or contact us at info@interxion.com for a free one-to-one workshop or expert consultation.



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. WP-ENT-HQ-PHYSICAL-IE-eng-4/20