Moving to the Cloud:
Security Without Sacrificing Performance

The digital transformation of the enterprise is in full swing—and cloud services are a foundational piece of this process. Cloud adoption continues to accelerate at an explosive pace, right alongside rising investments in cybersecurity.

According to IDG's 2016 **Enterprise Cloud Computing Survey,** 70% of organizations already use cloud-based applications and infrastructure and have dedicated 28% of their 2017 budget to cloud computing. These investments are spread across public, private, and hybrid cloud services. While all areas of adoption continue to climb, Gartner predicts that hybrid cloud use among Global 2000 enterprises will increase dramatically: from 10%–15% in 2015 to 25%–30% by 2019.

As enterprises integrate hybrid cloud services into their IT environments, many are facing a challenging mix of vendors and hosted services. This sometimes causes IT leaders to direct too many resources toward securing a unified infrastructure, diminishing the potential benefits of their cloud migration.

The new hybrid environment also comes with concerns about data privacy and security. Most enterprises are increasing their focus—and spending—in this area, according to CSO. The **2017 Global State of Information Security Survey** found that 59% of enterprises will increase security spending in response to increasing digitization and 62% rely on managed services for privacy and security. The **2017 State of the Network study** found that 71% of network teams correspond with their IT security team daily or weekly, showing how inseparable the dual priorities of performance and security are to the enterprise.

To satisfy these interrelated goals, IT leaders must create a proven hybrid architecture that supports the goals of digital transformation and that delivers enterprise-ready performance without sacrificing security—and vice versa.

Interconnection Oriented Architecture (IOA) is a proven design and implementation methodology that empowers IT organizations to deliver cloud-based services. IOA helps them meet three main performance/security objectives: First, reduce the distance between applications and workloads and end users; second, position data in a location adjacent to cloud compute; and third, enable interconnection with multiclouds and ecosystems.

IOA is imperative for enterprises that want to leverage the flexibility and enormous capacity of cloud computing for their large and sometimes distributed data sets. It is also vital for companies in tightly regulated industries such as financial services and healthcare or those working with sensitive information. In this second case, organizations can keep strategic data private for security and move less critical systems and data to the cloud for greater efficiency. IOA is a far better solution over a hub-and-spoke network that has costly legacy drawbacks such as complexity and security issues.

It's a Long Way to the Network Edge

The average organization in the 2016 IDG Enterprise Cloud Computing Survey spends 45% of its cloud computing budget on software as a service (SaaS), 30% on infrastructure as a service (IaaS), and 19% on platform as a service (PaaS). The remaining 6% is spread across storage, backup, disaster recovery, security, and other cloud services. These services span multiple cloud service providers.

The more cloud services a company leverages, the more it needs to integrate data and applications between the data center and the cloud as well as among differing clouds. However, this proliferation of cloud vendors makes it difficult for businesses—particularly Fortune 1000 companies—to provide customers and users with the performance and availability they require.

Moving workloads into the cloud increases the distance that data has to travel between on-premises systems and the network "edge," where most users—employees and customers alike—access the network. Basic physics dictates that the farther data has to travel from users across the corporate network, into the cloud, and back again, the greater the latency and degradation in performance.

In addition, the more cloud vendors a company uses, the more security risks it accumulates—for example, requiring employees to have multiple logins for multiple cloud solutions or needing separate application firewalls for each application in each cloud.

IOA addresses these challenges, by creating direct, secure connections among all the people, locations, clouds, and data in the organization, whether they're located on-premises or in a public or private cloud. This seamless level of integration provides a solid and secure foundation for a global digital platform that delivers the same performance for every user and application, regardless of location.

The Solution: A Three-Part Approach

Each organization will face its own challenges in deploying IOA, but the process generally requires these three key components:

1. **Communications/edge hub** – Bringing your applications and data closer to the customers, employees, and business partners who need access.
2. **Multicloud/ecosystem exchange** – Integrating and delivering your data via ecosystem exchanges that leverage multiple clouds and SaaS providers. This increases the speed of digital transformation/change by interconnecting all digital partners.
3. **Data hub** – Locating your data storage and compute resources in close physical proximity to each other.

The remainder of this paper focuses on the first component: shortening the distance between users and the cloud, as it provides the necessary foundation for the other two elements.

Closer to the Cloud

Moving workloads to the cloud puts distance between them and their users. Decreasing the distance to users again while still leveraging the cloud involves moving the organization's data center, with all its connections to SaaS and cloud-hosted software, to a colocation center that can link to multiple network and cloud providers via physical switches connected by fiber links. These interconnection points enable cloud providers to connect to their customers with minimal latency; combining the connections into a single interface makes them faster as well as easier to maintain and secure.

This type of solution mitigates many of the performance issues created by moving applications off-premises and splitting them among multiple clouds. It also helps ensure rich, consistent application delivery across private, public, and hybrid clouds, giving end users a predictable experience and helping IT maintain secure operations at scale.

In addition, requiring all traffic between the network and the cloud to pass through a single interface makes it easy to implement a cloud security gateway that examines, filters, secures, and directs all incoming and outbound traffic in real time. Users log in once to access all services, the IT team monitors and maintains one connection at the network edge, and traffic gets filtered once to protect all data.

CASE STUDY:
The First Step to Hybrid IT

To understand the cloud interconnection environment, consider a global digital company that began building its hybrid environment in 2014. After deciding to move all of its systems to the cloud, the company had two priorities: to protect productivity and limit latency by minimizing the distance between its users and the cloud and to ensure data security. When one cloud provider refused to let the company use its own intrusion prevention system and data loss prevention systems in the provider's cloud, the company opted to secure all of its workloads with F5 technology in the Equinix Interconnection Platform.

Equinix operates more than 150 data centers in 40 global markets. Twenty-one of these markets have Cloud Exchange facilities available. These enable enterprises to use interconnection services for making private, secure hardware connections to multiple clouds, including AWS, Microsoft Azure, Oracle Cloud, and others—all in a single location. F5 provides the intelligence layer for security and enhanced performance, with solutions that sit at the convergence of cloud and data center application services to deliver policing/security/logic technologies across both.

F5's BIG-IP platform cloud gateway services include single sign-on and ID federation as well as SSL inspection, DNS services, load balancing, a Web application firewall and an advanced data center firewall, and more. All these services are delivered in real time across all workloads, regardless of provider. This makes it possible to leverage the economics and services of each cloud while maintaining security and control of an application that's deployed in multiple clouds. This way developers can protect a single application in Azure and AWS with a Web application firewall that bridges both clouds and employees can sign on once to access all services, cloud-based or otherwise.

Leveraging cloud interconnection solved the digital industry company's latency problem. It also enabled the company to build its own infrastructure deployed with load balancing and security features rather than settling for what any individual cloud provider offered. These services include SSL inspection where an F5 BIG-IP platform decrypts and re-encrypts traffic and a third-party security service scans it for malware. This enables BIG-IP to move the company's DNS to the cloud without exposing the DNS itself to the Internet.

With strategic parts of their IT infrastructure now located in an Equinix Interconnection facility behind F5 cloud gateway services, the company knows which users are on their network and where those users are as they move into and out of applications. Instead of a private cloud, it can leverage the flexibility, scalability, tools, and speed of execution of AWS and Azure. The organization is also adding further authentication features by F5 for more-precise access and identity federation without vendor lock-in.

The Bottom Line

Despite being convinced of the power and cost-effectiveness of cloud services, many organizations take a piecemeal approach to moving to the cloud, creating individual connections to each cloud as they deploy. If they use an aggregator, it's often located at an on-premises data center, which makes management costly and complex while decreasing the performance of the very cloud services they want to boost efficiency.

Cloud interconnection in a Equinix facility is a vastly better alternative to managing a massive hub-and-spoke network that leads traffic back to a single location. It delivers the security and regulatory compliance of a managed facility with the added control of a single connection to multiple clouds and a single interface through which to manage them. By moving edge services off-premises, where the laws of physics place them closer to the cloud, companies can further recoup performance losses and connectivity expenses through increased agility.

Having direct, private access to multiple public clouds and cloud-based services in one location also helps avoid cloud provider lock-in. It provides negotiating leverage by making it simple to shift from one vendor or service to another and makes it easy to quickly add other services and applications that support faster business decision-making.

Finally, combining the cloud with hardware in a secure managed data center enables organizations to continue supporting legacy host systems that aren't cloud-ready or that can't easily be rearchitected for cloud implementation for technical or legal reasons.

Locating IT infrastructure in multiple environments (on premises, cloud edge, and within the cloud) can provide enterprises with levels of performance, security, and control they never thought possible before with hybrid cloud. Cloud interconnection improves identity management and access authentication, provides better visibility into network traffic, protects applications and data in the cloud—and prepares IT architecture for a truly hybrid future.

> To learn more about running F5 cloud gateway services on the globally available Equinix Interconnection Platform, visit:
>
> **www.F5.com/interconnect**
> **www.equinix.com/ioa**

About F5

F5 Networks (Nasdaq: FFIV) empowers organizations to successfully deliver, manage, and secure applications in the cloud with speed and agility—enabling them to embrace modern infrastructures without sacrificing traditional benefits and control.

www.f5.com

About Equinix

Equinix, Inc. (Nasdaq: EQIX) connects the world's leading businesses to their customers, employees, and partners inside the most interconnected data centers. In 41 markets across five continents, Equinix is where companies come together to realize new opportunities and accelerate their business, IT, and cloud strategies.

www.equinix.com

EQUINIX f5 CIO Strategic Marketing Services