WHITE PAPER

HorizonTek

SECURITY OF THE CLOUD

Enterprise IT is transitioning from the use of traditional on-premise data centers to hybrid cloud environments. As a result, we're experiencing a paradigm shift in the way we must think about and manage enterprise security.

From Four Walls to No Walls

Until now, the conventional view on IT security has been that applications and data are safe because they're physically housed within the confines of a company's data center walls using company-owned equipment. So, it's not surprising that many decision makers perceive greater risks as they trade physical assets for cloud-based solutions. Pre-cloud, data security focused on physical access and control, network security, and device threats. However, in the cloud world, OPEX infrastructure models are the norm. Corporate data constantly moves to/from company-owned equipment, to/from non-corporate devices, and it traverses both Layer 2 and Layer 3 network segments. IT personnel need to address encryption, authentication, and authorization (identity management) security strategies at the physical, data link, network, transport, session, presentation, and application layers.

The majority of the security budget once went to protecting the perimeter of the enterprise. Now, because of compliance mandates and the nature of cloud computing, security must be woven into every functional area of the company— from each business unit's infrastructure and line of business applications to externally sourced SaaS service agreements and identity management systems. Note that it's important to consider the dynamics of security within the cloud whether you adopt cloud-based application delivery or not.

CONSIDER THE DYNAMICS OF SECURITY WITHIN THE CLOUD

Business-Critical Computing in the Cloud

YOUR CHALLENGE: ADOPT CLOUD AND SECURE IT

Cloud computing opens up new avenues of collaboration, cost management, and convenience. Now you have a more agile way to deliver business-critical information with business partners, consumers, and end-users. You can minimize operational expenses by leveraging pooled resources and paying for just what you need, as you need it. And you can support the convenient mobile data access your users demand.

Business-critical computing on-premise

- Over-buying to meet highest anticipated demand
- Dedicated storage
- Dedicated compute
- Control: only the devices are mobile, not the apps
- Security budget dedicated to protecting the perimeter and controlling access

Business-critical computing in the cloud

- Pooled resources, scale on-demand
- Shared networking and compute in public clouds
- Delivery via the Internet in public clouds
- Security must be embedded within every layer and application when delivering via public infrastructure
- Private hosted clouds can be leveraged to deliver cloud economics without re-architecture

Cloud computing paves the way for IT advancements. But, without the proper cloud security mechanisms in place, your enterprise risks data leaks and security breaches. Cloud security fortifies IT efforts at every layer. The strength of that security depends upon the type of cloud you choose, the infrastructure supporting it, your service providers, and the identity management tools you use to collaborate with employees, partners, and consumers.

Security in Public, Private and Hybrid Clouds

Cloud computing can be divided into two general camps: public, in which the network, compute, and storage are multi-tenanted with little or no SLA on availability; and private, in which resources are dedicated, architected for high availability, and backed with SLA guarantees. When it comes to flexibility and economy, both types of cloud deliver with ease. When it comes to security, however, private clouds can offer significant advantages over public.

PUBLIC

The public cloud can be a hostile environment. You will have limited or no visibility into the underlying infrastructure and security controls. Nor will you have control over who's sharing your resources and the risks they could potentially introduce into the host system or data stores. Therefore, public clouds require a holistic approach to security: every component of the infrastructure must be secure and auditable in order to support business-critical computing and compliance.

Tips when considering public cloud

- Be wary of network QOS and DDOS mitigation. Your public cloud probably doesn't manage this for you.
- Be wary of noisy neighbor syndrome. Does your provider offer performance guarantees?
- Ensure adequate data security and firewalling of your environment.
- Ensure adequate authentication and security controls.

Fortunately, tools are being developed to give IT administrators back some level of control over data in public clouds. Citrix, NetApp, and VMware each offer forms of cloud-level data management. Citrix ShareFile, for example, provides a hybrid approach to public clouds. Data can live wherever it's needed but is always under the control of the ShareFile control plane. Data can't be shared without permission, and data that's managed remotely can be wiped clean no matter what device it's on.

PRIVATE

A private cloud is a virtualized datacenter within the cloud. Think of it as relocating your data center to an offsite location: you have dedicated compute, network, and storage resources that you manage as your own, just like you did on-premise. In this way, you can leverage the economics of the cloud without reworking business processes and applications to accommodate the rigorous security demands of public clouds. In the case of Faction's private hosted cloud, you can 'come as you are' and bring your own security (BYOS) or network (BYON) thanks in part to our Cloud's Faction-to-Faction Layer 2 Direct Connect service. Private clouds are especially advantageous to shops with tight regulatory requirements or limited resources.

Tips when considering private cloud

- Make sure your cloud provider lets you *bring your own* security capabilities. Don't settle for your provider's options; use yours. You've tested it. You use it. You trust it.
- Ask your provider about their private networking and vLAN capabilities. Ideally you want Layer 2 connections to/from your customer premise, data centers and from cloud to cloud. With Layer 2 you maintain network isolation and reduce complexities. At Faction, for example, customers can bring their network to our Cloud as-is. We eliminate the need to provision and manage complex firewalls, routers, and Spanning Tree Protocol [STP].

HYBRID

In some cases, the best methodology will command the resources of both private and public clouds. This hybrid approach supports the shift from traditional, singlesystem to multi-tiered application deployment. It also increases the available resources for test and development, business continuity, and managing resource demand spikes. To support data privacy and prevent leaks, all data moving between private and public clouds must be encrypted, and access to it must be tied to user identities.

Tips when considering hybrid cloud

- Ensure your cloud provider offers flexible usage of their storage and compute resources. In other words, if all you need is storage, does your cloud provider allow you to just buy storage?
- Determine whether your cloud provider gives you the ability to leverage existing tools, such as VMware APIs.
- Make sure your cloud provider allows you the ability to provision and leverage your existing vLAN topology. With Layer 2 private connectivity, you can use the same connection to access both public and private resources while maintaining network separation between public and private environments.

Fortunately, tools are being developed to give IT administrators back some level of control over data in public clouds. Citrix, NetApp, and VMware each offer forms of cloud-level data management. Citrix ShareFile, for example, provides a hybrid approach to public clouds. Data can live wherever it's needed but is always under the control of the ShareFile control plane. Data can't be shared without permission, and data that's managed remotely can be wiped clean no matter what device it's on.

PRIVACY AND SECURITY ARE THE LINCHPINS OF BUSINESS-CRITICAL COMPUTING

Compliance and the Cloud Service Provider

Whichever type of cloud strategy you choose—public, private or a combination of both—your cloud provider will play a key role in its success. You'll have many factors to consider in selecting your provider, but for the purposes of this paper, we'll focus on compliance, since customer privacy and data security are the linchpins of business-critical computing for many industries. (For more insight into the many factors to consider, read our whitepaper, Tips for Selecting Your Cloud Service Provider.)

To make sure the service provider can live up to the promises they're making, ask for the results of a third-party compliance audit. Look for audit capabilities like SSAE-16 SOC 1/2 and the ability to ink HIPAA Business Associate Agreements (BAA). Many agreements are multi-layered these days, so a key differentiator among cloud providers is their ability and willingness to work with consulting firms and other business entities to execute on these agreements.

Keep in mind that certifications are often only a stepping stone to actual audit performance. Be sure the provider has the personnel to support your audits and is willing to adapt to your individual needs rather than dictating how you should approach security. If you can take advantage of a provider's ability to be flexible with Layer 2 networking, for example, you'll benefit from a compliance cost standpoint because it allows you to recoup your network and security architecture investment and limit your exposure to risk by minimizing technology changes and subsequent process change.

Identity Management and Application Integration

Adopting applications in the new world of the cloud isn't just a matter of selecting the best applications to get the job done. Now you need to figure out how each application will integrate with your authentication (identity management) requirements. For example, requiring users to maintain multiple logins for multiple applications often negates the convenience factor of cloud access and injects new risks. From a human interaction standpoint, it erodes efficiency and security (who can remember all those logins and passwords without writing them down somewhere?). Instead, use identity management tools to rapidly provision and deprovision users while maintaining the convenience of simple logon processes. There are a variety of ways to achieve a secure hybrid cloud deployment.

Methods for securing hybrid cloud deployments:

- Use secure file sharing tools to allow data sharing while controlling compliance
- Use identity management tools to rapidly provision and de-provision users
- Implement single sign-on (SSO) to eliminate password proliferation and the associated risks
- Utilize multi-factor authentication mechanisms as required
- Integrate new applications with identity management systems
- Drive higher levels of access control to data and databases

As we tear down the walls protecting the perimeter of our enterprises and open new conduits to communication, collaboration, and mobility, most IT departments have moved security and data privacy to the top of their priority lists. And for good reasons: maintaining compliance, protecting reputations, and improving workforce productivity to name a few. Fortunately, security and cloud computing aren't mutually exclusive. Secure cloud computing can be achieved with the proper tools, service providers, business associate agreements, and the deliberate integration of applications and enterprise-wide identity management systems.

About Faction

Faction is an enterprise-class IaaS cloud service provider offering private, public, & hybrid cloud solutions through channel partners. At Faction we supply cloud the way you want it with extreme performance, deep control, and broad customization capabilities. When you join the Faction fold, you take back the keys to your kingdom. Reign as supreme commander in chief of your cloud. No compromises. No exceptions.

Faction is the only cloud that offers patented plug-and-play direct connections (via layer 2) into its cloud resulting in huge time savings (no time spent re-configuring everything)! With Type II SSAE 16 and SOC 1 & 2 compliant cloud nodes in eight geographies across the United States and in Europe (Seattle, Santa Clara, Denver, Chicago, Atlanta, New Jersey, New York, and the United Kingdom), Faction offers both Cisco UCS and Open Compute platforms, is a Platinum-level NetApp Service Provider, and is VMware vCloud® Powered. For more information, visit **www.factioninc.com** or call (855) 532-4734.

RICK VINCENT

DIRECTOR OF SOLUTIONS ENGINEERING

About the Author

As Director of Solution Engineering for Faction, Richard Vincent is responsible for architecting robust IAAS solutions, for channel partners and enterprises, enabling them to conduct business with compelling differentiation. Prior to joining Faction, Mr. Vincent served as a Storage Solution Executive at Dell, performed as an independent cloud consultant, and held the position of Director, Data Center Computing for Global Technology Resources, Inc GTRI. Mr. Vincent is a graduate of the University of Georgia, College of Business and is fluent in the Japenese language.

www.horizontek.com
888-972-7489