WHITE PAPER

McAfee
Together is power.

A Cloud Security Primer

A Cloud Security Primer

Despite the rapid proliferation of cloud computing, there's no single, standard blueprint for how enterprises are deploying and utilizing cloud models. Organizations are using private and public clouds, and often combining the two in hybrid clouds. They are deploying software as a service (SaaS), infrastructure as a service (IaaS) and platform as a service (PaaS) models. Some IT teams are delivering business-critical applications in a single private cloud; others are using multiple clouds for the same types of applications. Some are sanctioning shadow IT initiatives; others are discouraging them.

As diverse as your cloud environment may be, if you are involved in overseeing or deploying cloud services at your organization, there is one inviolable truism you must keep in mind at all times: No matter how simple or complex your cloud deployments, you can never allow the security of your data or applications to be compromised in any way. If there is a breach or cyberattack where your data is exposed, or if regulators cite you for non-compliance, it won't do you much good to point fingers at a public cloud provider. In the end, you are accountable for your own security—even if your public cloud provider has a "shared responsibility" model.

In this era of diverse cloud deployments, what does that mean? As data and applications flow through multiple clouds—private, public and hybrid—how can you ensure protection at all times? When you are using a public cloud, where does your responsibility for security end and where does the provider's begin? Can you ensure there are no gaps in protection when applications and data leave the perimeter of your network? As you embrace new technologies for private clouds, such as a software-defined data center (SDDC), what must you know about additional risk exposure?

This white paper discusses the security challenges of the different cloud models you may be deploying or considering. We also provide guidelines to help ensure that protection is not compromised no matter how diverse or complex you get in your use of cloud models. Finally, we offer a brief overview of some of the critical technologies that form the basis of a sound security foundation for the cloud era.

Security Challenges of the Different Cloud Models

It is not a stretch to say that cloud changes everything, particularly when it comes to security. Cloud computing presents security challenges that are quite different from the challenges of the past, even the recent past. For security professionals, it's not just about securing the perimeter, creating a DMZ or using the latest antivirus or antimalware products: It's about having an end-to-end security strategy that enables new levels of visibility, insight, control and protection—particularly as applications and data move fluidly across increasingly heterogeneous environments. Here are the key challenges presented by each of the various cloud models:

Hybrid Cloud

Hybrid cloud is a cloud computing environment that uses a mix of on-premises private cloud and third-party public cloud services with orchestration between the two platforms.[1] Organizations are increasingly using hybrid cloud models because they provide IT with flexible deployment models. Some business-critical applications can stay under IT control in a private cloud. Other applications may lend themselves to public cloud models to leverage benefits such as elastic scalability, cost savings or self-service provisioning.

Hybrid clouds present very specific security challenges because data and applications can flow in and out of various cloud environments: from your data center, into public clouds, and then back onto your network again. When your applications and data flow into the infrastructure of a public cloud provider, you run the risk of losing visibility and control. This can become an insertion point for malware. The challenge is to not only extend visibility across all computing resources—on-premises and in the public cloud—but to also apply consistent monitoring, protection, reporting and remediation across the entire end-to-end hybrid cloud environment.

What you need for hybrid cloud is an end-to-end security strategy that extends visibility and control. You need to easily apply protections and policies to all your virtual machines (VMs) no matter where they are located—within your private cloud or within the infrastructure
of a public cloud provider as part of your hybrid cloud environment.

Public Cloud

A public cloud is a cloud infrastructure that is open to use by the general public. It is owned, managed and operated by a business, academic or government organization, or some combination of them. It exists on the premises of the cloud provider.[2] From a security standpoint, the public cloud poses many of the same risks we just discussed in the section on hybrid cloud. Your data and applications are moving out of your visibility and control onto the infrastructure of a public cloud supplier. You have to know where your responsibilities end and where the responsibilities of your public cloud provider begin.

No matter how simple or complex your cloud deployments, you can never allow the security of your data or applications to be compromised in any way.

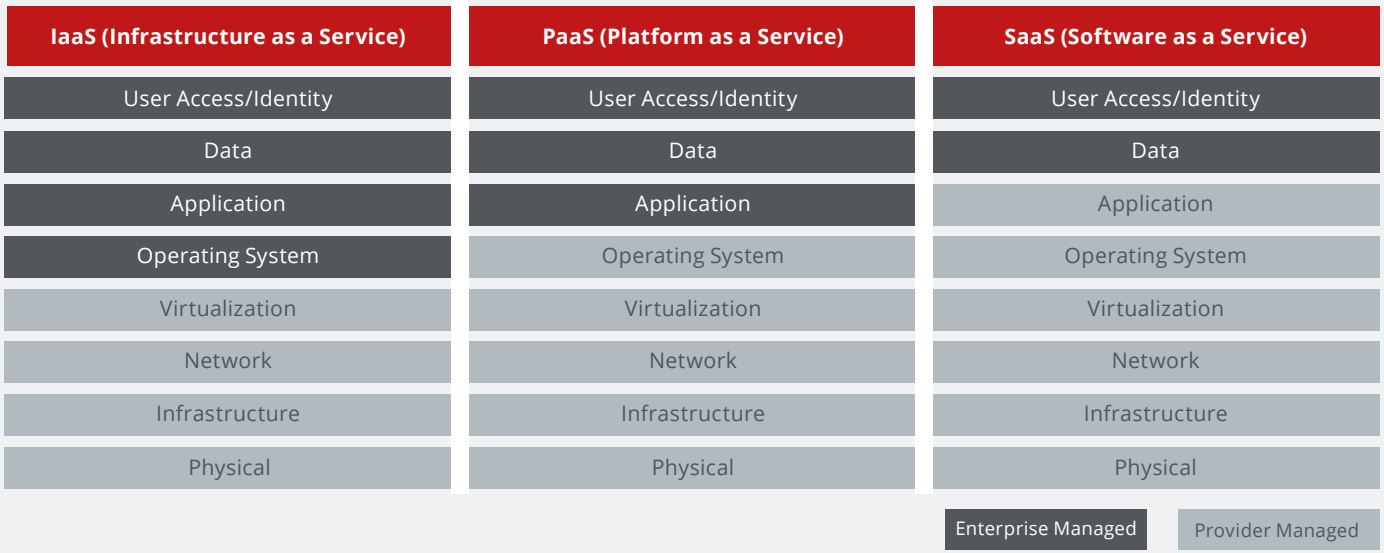
You can't just abdicate responsibility for security and compliance to the public cloud providers, assuming they will take care of it. You have to be fully aware of each cloud provider's shared responsibility model for each of the different cloud models you deploy: SaaS, PaaS and/or IaaS. Most of the major public cloud providers, such as Amazon, Google or Microsoft, detail their shared responsibility models on their websites. Take the time to understand these models and apply them to the various types of deployment models you may be using. And, before you sign any contracts, make sure responsibilities are spelled out on a case-by-case basis for each type of service.

An example of the public cloud shared responsibility model can be seen in the following graphic, in which the layers of the stack are differentiated by who is responsible for these items.

One of the biggest security challenges with public cloud is that it is so easy to deploy. A line-of-business manager or even an individual user can simply go to a public cloud supplier's website and sign up for a service with a few clicks and a credit card. This type of "shadow IT" deployment can expose the organization to incremental security risks. The IT team might not even know about it and the user may be unfamiliar with the types of security controls required to keep the company safe.

For security professionals, it's not just about securing the perimeter, creating a DMZ or using the latest antivirus or antimalware products: It's about having an end-to-end security strategy that enables new levels of visibility, insight, control and protection.

Shared Responsibility Model



One of the incremental challenges in dealing with public cloud is to gain an awareness of who in your organization is using public cloud services, what types of services they are using—SaaS, PaaS and/or IaaS—and how and when they are using them. Once you are able to attain this knowledge, you need to use technology solutions that enable you to exert some level of control over them, which will vary depending on the type of services in use. Referencing the shared security model, it is apparent that access, identity control and data protection should be top of mind for cloud security, especially with SaaS services. For IaaS environments, look for a security product that enables file integrity control and monitoring, which prohibits the installation of unauthorized software and monitors any changes that are made. Also, make sure you use a solution that provides host-based visibility into all of your applications.

Private Cloud

A private cloud is a type of cloud computing that delivers similar advantages to public cloud, including scalability and self-service provisioning, but through a proprietary architecture. Unlike public clouds, which deliver services to multiple organizations, a private cloud is dedicated to a single organization.[3]

The private cloud keeps data and applications under your organization's control so that they don't have to move out of your perimeter onto another provider's infrastructure. On the surface, this would seem to make security much simpler than either public or hybrid cloud deployments. In some ways that may be true, but as noted earlier, the cloud changes everything.

Private clouds require new deployment models for data centers that extend virtualization across the entire infrastructure and enable organizations to use cloud capabilities—resource pooling, elastic scalability, self-service capabilities and automatic chargebacks. This allows the business to benefit from a more service-centric IT model. This model, however, can bring incremental security risks that need to be anticipated and planned for.

One example: As virtualization expands within your data center beyond servers and into networks and storage, the amount of east/west traffic that flows between virtual machines (VMs) will increase dramatically. Legacy technologies focused on the perimeter will have no visibility into this traffic and will not be able to provide protection for them. You need the ability to apply security controls with deep packet inspection to all of this intra-VM traffic.

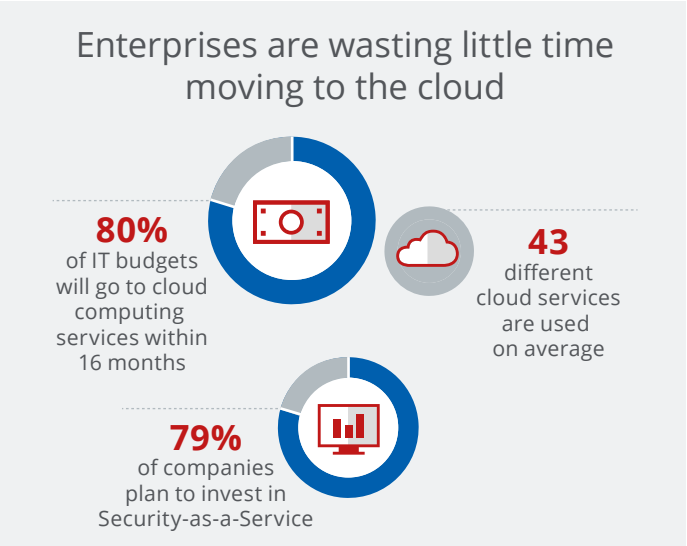
Another example: As new VMs are populated, you may experience security gaps if policies and protections are not applied to them immediately. You can't allow this to happen, so in the private cloud you need to be looking at applying security through a virtualized or software-defined model that leverages automation and orchestration of security policies. This will limit the time and risk involved in manual provisioning and deployments. If and when the VM moves, all of the security settings and protections should move automatically with it.

You can't just abdicate responsibility for security and compliance to the public cloud providers.

A third example: The dynamic nature of provisioning VMs and their overall load on servers in a private cloud environment can make capacity planning difficult. If you are running an antivirus solution that is not designed for the virtual environments within a private cloud, it can be an almost impossible task. Even though traditional antivirus will run on these VMs, the cumulative performance impact on the infrastructure will be enormously high. This will directly affect how many VMs can run on a server, thus impacting the designed VM-to-server ratio—and operational returns, as well. An optimized virtual antivirus solution will be better suited to protect this elastic environment without altering performance and scalability.

Taking the Next Step

The shift to cloud computing is one of the most significant IT initiatives of our time. IDC has said: "'Cloud First' will become the new mantra for enterprise IT."4 According to a recent State of Cloud Adoption report by McAfee, 80% of IT budgets will go into cloud computing services within the next 16 months, and 96% of organizations will increase their cloud investments.5 In addition, companies are using an average of 43 different cloud services, and 40% already process or store sensitive data in the cloud. And, while 77% of respondents said they trust the cloud more than they did a year ago, 66% also said they believe that senior management doesn't totally understand the risks of storing sensitive data in the cloud.

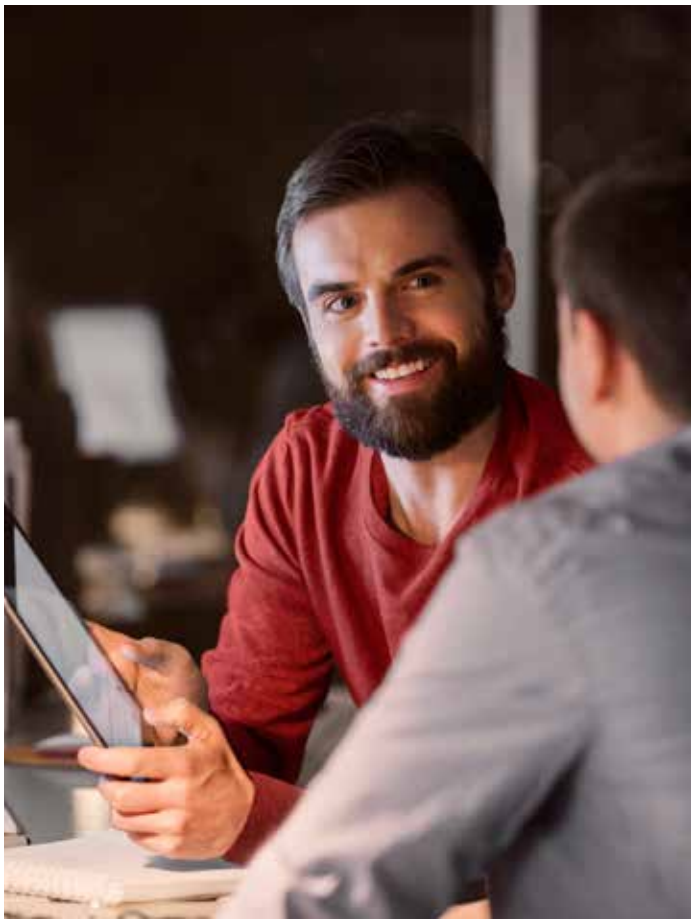


For security professionals, the cloud requires a new approach. Cloud security is an end-to-end challenge whereby the solutions must be built into the overall IT environment and not tacked on as an afterthought. IT and security teams must use tools and technologies that have been designed specifically to meet the challenges of the cloud era. Finally, these technologies and tools must be deployed as part of an integrated deployment model. You want to ensure that that protection is consistent across all cloud environments. Features such as threat detection and intrusion prevention must be delivered in real time to protect the entire organization at all times, no matter where data and applications are located.

Security solutions must be built into the overall IT environment and not tacked on as an afterthought. IT and security teams must use tools and technologies that have been designed specifically to meet the challenges of the cloud era.

In building your cloud security strategy, it is important to work with a vendor that offers an integrated model for cloud security, as well as a diverse set of cloud-specific solutions. Critical technologies you will need to deploy include a software-defined security controller; a virtual network security platform; virtual antimalware protection; host-based public cloud protection; advanced threat intelligence; and centralized management. These solutions, integrated with one another, will form the foundation of your cloud security strategy for now and into the future. And, as always seems to be the case in enterprise IT, the future is already at hand.

If you're ready to take the next step toward ensuring the security of your cloud environments, please contact McAfee at **www.mcafee.com/cloudsecurity**.



1. "**Hybrid Cloud**," **SearchCloudComputing**, TechTarget
2. "**The NIST Definition of Cloud Computing**," Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, September 2011
3. "**Private Cloud**," SearchCloudComputing," Tech Target
4. "**IDC Predicts the Emergence of 'the DX Economy'** in a Critical Period of Widespread Digital Transformation and Massive Scale Up of 3rd Platform Technologies in Every Industry," IDC, Nov. 4, 2015
5. "**Blue Skies Ahead? The State of Cloud Adoption**," McAfee, April 2016

About McAfee

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com