2018 White Paper

Security to the core: Top five considerations for securing the public cloud

Answers to pressing questions from IT architects on public cloud security

IBM **Cloud**

IBM

Two forces are coming head-to-head in today's world of information technology.

The first is the accelerating—and inexorable—adoption of public cloud at scale. The other is rapidly heightening sensitivity and awareness of the global data threat environment, which predictably has called into question the security of public cloud.

Thus, IT architects find themselves asking, "How do I mitigate security risks while still moving ahead with our ambitious public cloud plans?"

Data underscoring the interest in public cloud is unambiguous. A report from McKinsey & Co.[1] points out that "using the public cloud disrupts traditional cybersecurity models that many companies have built up over years." McKinsey's study of 90 enterprise-class organizations last year found that 80% plan on having 10% or more of their critical workloads in the public cloud by 2020, or double their current public cloud use today. Not surprisingly, the research and consulting firm urges organizations to "evolve their cybersecurity practices dramatically to consume public cloud services…to protect critical data."

The high cost of low security

Meanwhile, efforts to supercharge public cloud security efforts run headlong into a highly dynamic global threat environment. IT architects are understandably wary of the increasing scale and scope of the threats to Internet-facing applications, websites and workloads. Highly sophisticated and well-financed attackers are motivated to exploit what they perceive as vulnerabilities in public cloud and public application programming interfaces (APIs). And they are doing well. One recent study of more than 1,000 organizations revealed that 76% reported two or more distributed denial-of-service (DDoS) attacks in the previous year.[2] The average cost of a U.S. data breach has crested $7 million, with estimates of a successful DDoS attack topping $250,000 per hour.

The secure pathway ahead

The significant business benefits of public cloud, as well as the potential threats to sensitive cloud data that cyberattackers are seeking to access, are clear. Here are the top 5 considerations that IT teams, CTOs and other business stakeholders should address when choosing among public cloud security solutions.

1. CHOOSING BARE METAL PROVIDES AN ISOLATED ENVIRONMENT.

Single-tenant bare metal servers are dedicated to the customer. Running workloads in an isolated environment adds an extra level of security for your workloads, but not all compute severs are the same when it comes to security. Be sure the solution is truly single tenant and dedicated solely to your organization so you get complete isolation. Some providers will place a hypervisor on a bare metal server, turning it into a virtual server, which distributes the workloads among different users. Seek a solution tailored to your needs.

2. NOT ALL PUBLIC CLOUD FIREWALLS ARE CREATED EQUAL.

IT architects recognize that firewalls are an integral part of protection for the cloud infrastructure, both from external cyberthreats and to help meet compliance requirements. As organizations transition from traditional on-premises appliances to software-as-a-service models, the right firewall can ensure you have the same security levels for both. Look for solutions with the greatest variety of options, such as instance-level protection; network-level protection from firewalls that can be deployed as high-availability options; dedicated hardware firewalls that protect ingress traffic on any or all servers on a single, public virtual LAN; both portal and API support to make it easier to get started; and next-gen features such as an intrusion protection system, antivirus and a web application firewall. Remember that while cloud-native firewall solutions are broadly available, physical appliances are still crucial for the enterprise. You don't want to have to choose between security and performance.

3. SECURITY GROUPS HAVE MANY AND VARIED RULES.

In the world of cloud security, security groups are sets of IP filter rules designed to regulate access to network resources. They define how to handle incoming (ingress) and outgoing (egress) traffic to both the public and private interfaces of a virtual server instance. It's worth noting that you can assign security groups to a single or multiple virtual server instances. Be sure the security groups available to you will adequately address key network security issues. For example, IT architects usually want to secure a virtual server immediately upon provisioning. So be sure you can use security groups at the time of ordering the virtual server to get complete control of the traffic passing through the server upon deployment. And look for a solution that does not charge extra for using the security groups feature, as you likely will want to use security groups for all virtual servers in need of protection at the solution provider's data centers.

4. ENCRYPTION KEYS ARE KEY TO SUCCESS.

The 1,000 global IT leaders polled in the study cited earlier were asked to choose from a list of factors that would increase their willingness to use public cloud services. At the top of that list was "encryption of my organization's data with the ability to store and manage encryption keys locally." Look for a cloud security solution featuring a tamper-resistant hardware device for securely storing cryptographic key material. Your keys should always remain in FIPS 140-2 Level 3-compliant hardware. Such security modules should allow IT teams to remotely manage them and be sharable among multiple applications or tenants to reduce audit and compliance costs. And if your use cases require high performance like protection of SSL/TLS keys and high-volume code signing, be sure the hardware module you choose can provide these.

5. EASE OF USE SHOULDN'T MEAN SACRIFICING PERFORMANCE OR SECURITY.

IT teams often bemoan cloud security solutions that force them to choose between security and performance. Instead, look to solutions that offer low-latency security services fully integrated with traffic optimization services, such as caching and load balancing. A solution focused on ease of use should allow you to secure web applications and websites within minutes while protecting against potentially costly misconfigurations.

Getting public cloud security right

Security should be a top priority when selecting a public cloud provider. According to Forbes, there is one top-three cloud service provider that continues to vault ahead of its competitors by leveraging its "highly successful emphasis on transforming its vast array of software expertise and technology from the on-premises world to the cloud."[3] That provider is IBM, whose public cloud customers gain access to not only the full measure of IBM Cloud security services, but also a massive global security team supporting thousands of customers around the world.

IBM's approach to securing the cloud focuses on providing optimal visibility to proactively monitor public cloud services, enabling users to respond to threats faster and greatly accelerate investigation and mitigation. In addition to sophisticated yet easy-to-use analytics, IBM solutions allow users to encrypt data both at rest and in motion with a key management service. It also offers identity and access management capabilities to reinforce compliance management and reduce overall risk.

Some essential public cloud security solutions and services from IBM include:

Bare metal server solutions that deliver security in the form of isolated environments plus the added benefit of complete control and flexibility. With IBM Cloud bare metal servers, customers never share compute resources. Rather, you own the entire stack, including configuring and customizing the components. That means you don't have to worry about "noisy neighbors" sharing resources and slowing your workloads.

Firewalls that enable seamless transitions from traditional to virtual environments. Key among such IBM offerings is the **FortiGate Security Appliance**, FSA 10Gbps, the first enterprise-grade, hardware-accelerated, high-throughput firewall.

Cloud security groups that let users secure a virtual server immediately upon provisioning while delivering highly granular control over traffic at an instance level.

A hardware security module that locks down the customer's cryptographic infrastructure by securely managing, processing and storing cryptographic keys inside a tamper-resistant, tamper-evident device.

Cloud Internet Services, a software-defined security solution that provides security, resiliency and performance capabilities for your web-facing applications. With a few simple clicks or commands from within a single portal or API, a faster, more secure Internet experience awaits.

Conclusion

Public cloud at scale is attainable today without putting sensitive data at unnecessary risk. While there are many service providers offering a dizzying array of public cloud services, you must carefully scrutinize and compare these services before making public cloud bets. As the most experienced global leader in enterprise security among all top public cloud providers, IBM Cloud has both the services and the security team to give your business what it wants most: security to the core of the infrastructure—and peace of mind.

For more information, please visit
https://www.ibm.com/cloud/security

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America 2018

Footnotes

1 “Making a Secure Transition to the Public Cloud,” McKinsey & Co., January 2018

2 “IBM Cloud Internet Services: Optimizing Security to Protect Your Web Applications,” IBM, February 2018

3 “The Top 5 Cloud-Computing Vendors,” Forbes, Nov. 7, 2017

TechTarget | Custom Media