Solution Brief

Embrace Public Clouds with Confidence.

Secure your servers no matter where they are.

Convenient, flexible, easy to manage, and budget friendly—these are some of the predominant reasons behind the rush to embrace public cloud services like Amazon Web Services (AWS), Microsoft Azure, and others. This innovative new technology trend makes a great deal of sense for forward-thinking enterprises that value agility, and it is rapidly gaining ground as an attractive alternative to private clouds or on-premises physical servers. In its *2014 State of the Cloud Survey*, RightScale reported that 87% of participants are currently using public cloud services like AWS, Microsoft Azure, and others.[1] The advantages of using public cloud servers are many. They provide a secure and compliant infrastructure, which is often difficult to achieve in a private cloud without a huge investment. Organizations can move data and applications as needed from on-premises servers to the public cloud. Start-up developers, whose needs may fluctuate on a day-to-day basis, can easily scale up or down in minutes, as required. Some providers offer redundancy options within and across regions and even globally. Finally, the financial benefits are significant—since usage is billed hourly, costs can be shifted from capital expenditures to operational expenditures.[2]

Security Is a Shared Responsibility

Can you put your trust in public cloud servers? Many organizations and sectors do and have already made the big leap. According to Tech Republic blogger Kris Bliesner, the US government is the biggest cloud user worldwide—with more than 50% of its government computing operations on public clouds. At 64%, banking, not social media or gaming, as you might expect, leads in the amount of activity generated in the cloud.[3]

Contrary to popular belief, many large public cloud server infrastructures are actually quite well fortified—often more so than their customers' infrastructure. Of course, the level of security you might require varies according the applications and data you intend to access. Websites, development and testing tools, documentation, and other common enterprise applications and data are a good choice for public cloud servers, as they may not require strict security. Public cloud infrastructure security, which may meet or exceed your expectations, is clearly the responsibility of

intel Security

the providers. But, bear in mind that, when it comes to protecting the assets you choose to move to these servers, the ball is clearly in your court. Amazon states this upfront: "AWS has secured the underlying infrastructure, and you must secure anything you put on the infrastructure or connect to the infrastructure."[4] This is not meant to inspire fear, uncertainty, and doubt, but rather to put you in charge of your own security. There's no need to sacrifice security for convenience and cost savings of public cloud servers. Intel Security can help you make your public cloud servers as safe and manageable as your on-premises servers with McAfee® Public Cloud Server Suite.

Public Cloud Security Challenges

While it's reassuring to know that most public cloud providers stay on top of security updates and maintain a stable security posture on the infrastructure level, organizations that use these services need to address the security of their own assets, as AWS affirms.

You can't protect what you can't see.

To feel confident that your data and applications are safe in the public cloud, you need to be able to see each and every workload instance as it's created. But there are several obstacles that get in the way of complete visibility into public cloud activities. First, usage is variable, so there's a lot of "noise" in public cloud servers. It's not unusual for new server instances to appear on a daily basis within the public cloud, and some are abandoned and become "zombies" that are hard to track down. There's also the issue of "shadow IT," where users interact with the cloud directly without authorization. Finally, your organization might be running web applications that scale automatically according to user demand, and these can be difficult to monitor.

It's all about the data.

You take painstaking measures to safeguard precious corporate data for on-premises servers. What about the data you store and use in the public cloud? Traditional network and perimeter security tools are not an option for the public cloud, as they can't be bolted on. You can consider virtual appliances, but often they don't integrate with hypervisors and can become bottlenecks when you need to scale up your cloud servers. Unauthorized access to your critical data by cloud providers and third parties is another concern. To truly minimize the threat of malware and botnets, encryption is essential and should be a top security priority for companies using the public cloud.

How do we manage the public cloud?

Most enterprise IT departments are already overloaded, so the last thing you want to do is make their already long days even longer or hire more staff members to manage your public servers—especially since reducing your capital expenditures was one of the reasons that you chose the public cloud to begin with. Instead of eroding your potential savings or putting IT in overdrive, the ideal choice is a simple management platform that allows you to manage all your servers—physical, virtual, in your private cloud, or in a public cloud.

In-Depth Public Cloud Security

Intel Security quells any trepidation you might have with respect to protecting your public cloud servers with McAfee Public Cloud Server Security Suite. This comprehensive, host-based security solution offers complete visibility into all of your server instances across public cloud infrastructures such as Amazon AWS and Microsoft Azure. It provides the same tough antivirus and intrusion protection capabilities found in our other server security suite solutions, and convenient, centralized management with the familiar McAfee® ePolicy Orchestrator® (McAfee ePO™) console.

Figure 1. McAfee Public Cloud Server Security Suites provide insights, unified protection, and centralized management for public cloud workloads.

Enhance visibility with cloud connectors.
McAfee Data Center Connectors are part of McAfee Public Cloud Server Security Suite and enable you to see everything that's running within an Amazon AWS, Microsoft Azure, or OpenStack environment. These plug-and-play add-ons help you automatically discover, manage, and protect all of your cloud instances. And you no longer have to worry about the potential security threats posed by shadow IT. McAfee Data Center Connectors provide visibility of server instances at the time they are provisioned and help you automatically apply security policies and critical protections. Now your public cloud-based servers can have the identical robust security posture as your on-premises servers.

Secure your public cloud servers from every angle.
McAfee Public Cloud Server Security Suite addresses nearly every aspect of public cloud security—from powerful top-rated antivirus to application whitelisting to all-important encryption. The capabilities in this suite mirror the same level of protection we extend to your physical servers, supporting both Windows and Linux.

- **McAfee VirusScan® Enterprise for Servers:** Ranked number one by NSS Labs against day-zero exploits and evasion attacks,[5] this technology maximizes your defense against all types of malware—viruses, worms, Trojans, and more. It scans your server instances in the public cloud in real time to proactively safeguard your workloads from known and emerging threats. This protection is available for both Linux- and Windows-based server instances in the public cloud.
- **Host-based intrusion prevention:** Now you can defend your public cloud instances against complex security threats that may inadvertently pass through. Peace of mind comes from knowing that McAfee Global Threat Intelligence provides up-to-date information on network connection reputation to protect servers against advanced threats, botnets, and denial-of-service (DoS) attacks.
- **Firewall for Linux and Windows:** Prevent malware from entering and propagating to public cloud servers by examining network traffic packets against rule sets that determine what is allowable and what is not.
- **Application control:** Dynamic whitelisting prevents unwanted code from executing on your public cloud servers by prohibiting installation of unauthorized software. McAfee Application Control for Servers uses a dynamic trust model and innovative security features that thwart advanced persistent threats without requiring signature updates or labor-intensive list management. This ensures that your server instances in the public cloud are kept to a known, secure footprint.

- **File Integrity monitoring (change control):** This capability continuously detects system-level changes in the public cloud and prevents tampering by blocking ad hoc or unauthorized changes to system files, directories, and configurations.
- **Data protection for the cloud:** Encryption is essential for protecting vital corporate data and intellectual property that traverses or is stored on public cloud servers. With a few simple clicks, McAfee data protection for the cloud will discover Amazon EBS storage volumes and improve their security posture by encrypting them.

A single console eases management.
Our unique, industry-leading McAfee ePO console gives you single-pane manageability for physical and virtual servers, including servers in the private and public cloud, for enhanced visibility across your entire IT infrastructure. The McAfee ePO agent enforces policies for public cloud server instances to ensure best practices, executes tasks like updating protections, and collects and sends event information at intervals to the McAfee ePO server so that appropriate action can be taken when threats strike. It's the centralized hub for a broad range of Intel Security products—data protection, email and web security, and risk and compliance tools. And, because of its open, scalable architecture, McAfee ePO software enables you to leverage security products of more than 100 partner companies.

The intuitive, interactive interface features web-based, customizable dashboards, a drag-and-drop environment, and built-in reporting tools make the job of managing public cloud servers easier, and less time consuming for IT. There's no need to invest in additional headcount or management servers.

Flexible pricing benefits your bottom line.
One of the big reasons enterprises are migrating their computing operations to the public cloud is to cut costs and shift from capital expense budgets to operating expense budgets. Pricing for McAfee Public Cloud Server Security Suite aligns with that objective. Priced by the hour, it gives you the flexibility to pay for security in a way that meets the needs of your organization. The suite approach, which unifies advanced security capabilities, also makes this a cost-effective investment, ultimately lowering operational expenses related to remediating security issues.

Summary

As you take the next step on the road to public cloud adoption, you can do so with confidence. McAfee Public Cloud Server Security Suite provides advanced security capabilities unified in a single suite with a centralized management console. Best of all, McAfee Public Cloud Server Security Suite fully complements your cloud strategy and supports your goals from every perspective—IT, business, and financial.

1. *RightScale 2014 State of the Cloud Survey*, **www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2014-state-cloud-survey**
2. **http://www.techrepublic.com/blog/the-enterprise-cloud/private-vs-public-cloud-why-the-supposed-debate-is-really-no-debate-at-all/**
3. **http://www.techrepublic.com/blog/the-enterprise-cloud/private-vs-public-cloud-why-the-supposed-debate-is-really-no-debate-at-all/**
4. **http://aws.amazon.com/security/**
5. **http://www.mcafee.com/us/resources/reports/rp-nss-labs-corporate-exploit-evasion-defenses.pdf**

61894brf_pcs_0415_ETMG

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com