Firebox Cloud on AWS

Extending the WatchGuard security perimeter to protect business-critical assets in AWS

What is Amazon Web Services (AWS)?

AWS is a platform that allows you to quickly and easily deploy resources in the public cloud. As an Infrastructure-as-a-Service (IaaS) offering, customers build systems in a hosted environment that provides compute, storage, content delivery and other functionality for increased flexibility, scalability and reliability. AWS enables you to avoid capital infrastructure costs with a pay-as-you-go model that makes the public cloud an appealing alternative to on-premises datacenters, even among small and midsize businesses. In fact, according to RightScale's 2016 State of the Cloud report, 71 percent of small and midsize businesses (SMBs) are running at least one application in a public cloud environment. However, moving infrastructure outside of on-premises datacenters that you control changes the security dynamic, and necessitates the use of additional security solutions to keep your assets safe.

Security in the Public Cloud

While the public cloud provides countless new opportunities for businesses big and small, it's continued growth has also made it a major focus for criminal hackers. Hackers have begun to target or infect servers running in public cloud services, and there have even been cases where hackers have taken over servers running in Amazon EC2 – the virtualized compute portion of AWS.

> From a security perspective the servers you spin up in public cloud environments, like AWS, are no different than those in your own datacenter. If you leave a port open, without a firewall or access control rules, hackers can attack it in the same way they attack physical servers.

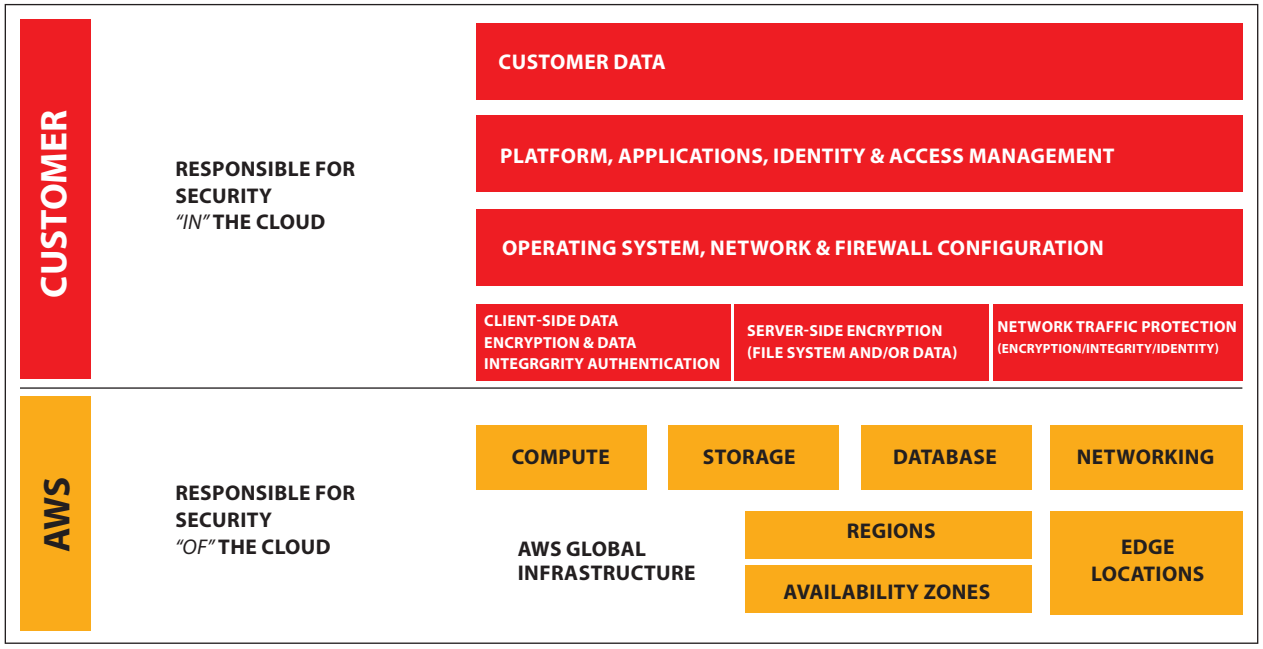
In short, without the proper protections, attackers can hack servers in the public cloud just as easily as the ones on your premises. As we move more and more of our data to IaaS servers, you can expect criminal hackers to follow. With so much at stake, AWS has gone to great lengths to ensure the security of their cloud infrastructure, but the protection of sensitive assets in the public cloud make security a shared responsibility.

Security and the AWS Shared Responsibility Model

Amazon Web Services takes pride in the security of their cloud infrastructure but they make it clear that the security of your business-critical assets in the cloud is your responsibility. Under the AWS Shared Responsibility Model, AWS makes a distinction between:

- Security measures that the cloud service provider (AWS) implements and operates – "security OF the cloud"
- Security measures that the customer implements and operates, related to the security of customer content and applications that make use of AWS services – "security IN the cloud"

AWS manages the security OF their cloud through a series of security tools that protect their endpoints, provide encryption of stored data, and effectively segregate the virtual networks and applications of their customers. Under the shared responsibility model you remain in control of the security approach to your content, platform, applications and networks.



Enhancing the Security of AWS with Network Security

AWS provides built-in virtual firewall functionality that controls access to instances and VPCs (Virtual Public Clouds). Called network access control list (ACL), this optional layer of security acts as a firewall for controlling traffic in and out of one or more subnets. But controlling access only solves a small portion of the security challenge. For trusted security in AWS, customers need the ability to inspect inbound and outbound traffic with a robust set of security tools designed to detect and prevent modern cyber attacks.

Holding Up Your End of the Bargain in the AWS Shared Responsibility Model with Firebox Cloud

WatchGuard Firebox® Cloud brings the protection of WatchGuard's leading Firebox® UTM appliances to the public cloud. With Firebox Cloud for AWS, your AWS environment is protected by comprehensive portfolio of security services, from traditional intrusion prevention, gateway antivirus, application control, and URL filtering, to more advanced services for protecting against evolving malware, ransomware, and data breaches. Each security service is delivered as an integrated solution within an easy-to-manage and cost-effective virtual Firebox.

What's more, WatchGuard Firebox Cloud is completely compatible with WatchGuard Dimension, a cloud-ready network security visibility solution that comes standard with WatchGuard's flagship Unified Threat Management and Next Generation Firewall platform. Dimension provides a suite of big data visibility and reporting tools that instantly identify and distill key security issues and trends, and deliver valuable insights to set meaningful security policies across all of your environments, making managing the security of your AWS environment a snap.

Top Firebox Cloud Use Cases

- **Protect Servers Deployed on AWS.** To provide protection to one or more virtual servers that are accessible from the Internet, you can install a Firebox Cloud instance. Your instance of Firebox Cloud is then the gateway for inbound connections to your servers from the Internet. You configure policies and security services on your instance of Firebox Cloud to control traffic to your virtual servers.
- **Branch Office VPN Gateway.** A Branch Office Virtual Private Network (BOVPN) enables organizations to deliver secure, encrypted connectivity between geographically separated offices. The networks and hosts on a BOVPN tunnel can be corporate headquarters, branch offices, remote users, or telecommuters. These communications often contain the types of critical data exchanged inside a corporate firewall. In this scenario, a BOVPN provides confidential connections between these offices. This streamlines communication, reduces the cost of dedicated lines, and maintains security at each endpoint. You can configure your Firebox Cloud as a branch office VPN (BOVPN) gateway endpoint so you can maintain a secure VPN connection between your AWS network resources and other networks protected by a Firebox or compatible VPN gateway endpoint.
- **Mobile VPN Gateway.** You can also enable Firebox Cloud to accept VPN connections from SSL, IPSec, and L2TP mobile VPN clients, and configure policies to control user and group access to your protected AWS network resources.

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, endpoint security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by over 18,000 security resellers and service providers to protect 250,000 customers. WatchGuard's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for midmarket businesses and distributed enterprises. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit **WatchGuard.com**.

For additional information, promotions and updates, follow WatchGuard on Twitter @WatchGuard, on Facebook, or on the LinkedIn Company page. Also, visit our InfoSec blog, Secplicity, for real-time information about the latest threats and how to cope with them at **www.secplicity.org**.

WatchGuard®

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com