ALERT LOGIC®

IT'S NOT YOU, IT'S ME:

UNDERSTANDING THE SHARED RESPONSIBILITY OF CLOUD SECURITY

Cyber attacks are on the rise. Companies both large and small are targeted daily by hackers seeking valuable data to monetize in the cyber underground. Recent reports show that 87% of organisations are making use of cloud infrastructure[1], while analysts predict spending will exceed $200 billion[2] in 2016. This means: 1) Organisations are making use of public clouds now more than ever before, and 2) Hackers now have a larger attack surface to gain access to sensitive data. It is now imperative for organisations to understand the attack methods being used to compromise their environments, so they can prepare a defence strategy when they become the target of an attack.

In Alert Logic's Cloud Security Report 2015, top cyberattacks methods aimed at cloud deployment grew with web application attacks, brute force and suspicious activity being the most pronounced. This is not surprising – production workloads, applications and valuable data are shifting to cloud environments, and so are the attacks. Hackers, like everyone else, have a limited amount of time to complete their "job". They want to invest their time and resources into attacks that will bear the most fruit: Their hypothesis, which in some cases may be true, is that businesses have a misconception about the security they need in the cloud. Some businesses, attackers have found, mistakenly assume cloud providers take care of all their security needs. The reality, however is that security in the cloud is a shared responsibility.

TOP THREE INCIDENT CLASSES

CLOUD ENVIRONMENTS YEAR-OVER-YEAR COMPARISONS

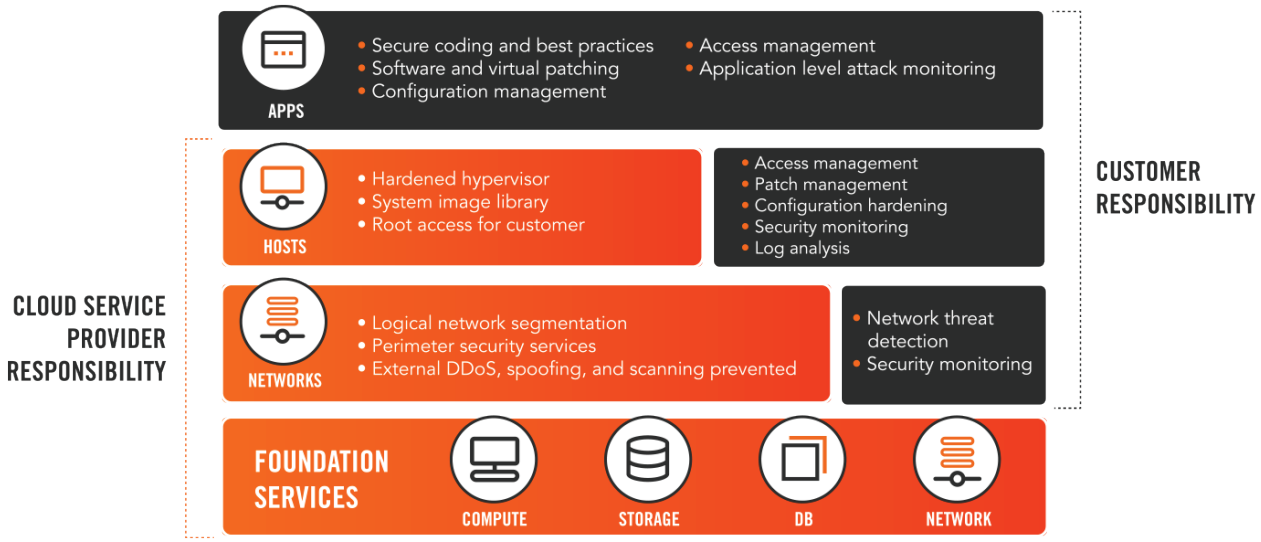
1 http://www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2014-state-cloud-survey
2 http://allthingsd.com/20120709/public-cloud-and-telecom-to-lead-3-6-trillion-in-it-spending-this-year-garner-says/

UNDERSTANDING SHARED SECURITY RESPONSIBILITY

In the public cloud, a key to being secure is a solid understanding of the shared security model that exists between you (the customer) and your cloud provider. Without this, you may make assumptions that your cloud provider is protecting you, when in fact you are actually responsible for particular security functions.

Your cloud provider is responsible for securing the fundamentals services, such as computer power, storage, database and networking services, but you will be responsible for the configuration of these services. At the network layer, your service provider is responsible for network segmentation, perimeter services, some DDOS and spoofing.

But you are responsible for network threat detection, reporting and any incident reporting. At the host layer, you are responsible for access management, patch management configuration hardening, security monitoring and log analysis. The application security components of your site are 100% your responsible. The model below shows a breakdown of responsibilities between you and your service provider:



Understanding your role and the role of your cloud provider will not only help you make the best decision concerning your cloud infrastructure, it will also ensure that once implemented your cybersecurity strategy will efficiently and cost-effectively protect your data from threats to the cloud.

SEVEN BEST PRACTICES FOR CLOUD SECURITY

There are seven key best practices for cloud security that you should implement in order to protect yourself from the next vulnerability and/or wide scale attack:

1. SECURE YOUR CODE

Securing code is 100% your responsibility, and hackers are constantly looking for ways to compromise your applications. Ensure that your code is fully tested and secure, and that security is an integral part of your development lifecycle, not bolted on as an afterthought.

2. CREATE AN ACCESS MANAGEMENT POLICY

The lack of a physical perimeter in the cloud means thinking differently about access management, logins are the keys to your kingdom and should be treated as such. Do you have a strong access management policy in place? Especially concerning those who are granted access on a temporary basis? Integration of all applications and cloud environments into your corporate AD or LDAP centralized authentication model will help with this process as will two factor authentication.

3. ADOPT A PATCH MANAGEMENT APPROACH

Unpatched software is one of the first things a hacker looks for you, yet too many users postpone or ignore patches. Keep your environment secure by outlining a process where you update yours systems on a regular basis. Consider developing a checking of important procedures, test all updates to confirm that they do not damage or create vulnerabilities before implementation into your live environment.

4. LOG MANAGEMENT

Log reviews should be an essential component of your organizations security protocols. Logs are now useful for far more than compliance, they become a powerful security tool. You can use log data to monitor for malicious activity and forensic investigation.

5. BUILD A SECURITY TOOLKIT

No single piece of software is going to handle all of your security needs. You have to implement a defence-in-depth strategy that covers all your responsibilities in the stack. Implement IP tables, web application firewalls, antivirus, intrusion detection, encryption and log management.

6. STAY INFORMED

Stay informed of the latest vulnerabilities that may affect you, the internet is a wealth of information. Use it to your advantage, search for the breaches and exploits that are happening in your industry.

7. UNDERSTAND YOUR CLOUD SERVICE PROVIDER SECURITY MODEL

Finally, as discussed get to know your provider and understand where the lines are drawn, and plan accordingly.

Cyber attacks are going to happen; vulnerabilities and exploits are going to be identified. By having a solid security in depth strategy, coupled with the right tools and people that understand how to respond you will out you into a position to minimise your exposure and risk.