SEVEN BEST PRACTICES OF CLOUD SECURITY

01 **SECURE YOUR CODE**
Hackers are continually looking for ways to compromise your applications. Code that has not been thoroughly tested and secure makes it all the more easy for them to do harm. By testing your libraries, scanning plugins and the like you can save yourself headaches down the road.

02 **CREATE ACCESS MANAGEMENT POLICIES**
Logins are the keys to your kingdom and should be treated as such. Make sure you have a solid access management policy in place, especially concerning those who are granted access on a temporary basis

03 **ADOPT A PATCH MANAGEMENT APPROACH**
Unpatched software and systems can lead to major issues for your organization. Keep your environment secure by outlining a process where you update your systems on a regular basis.

04 **REVIEW LOGS REGULARLY**
Log review should be an essential component of any organization's security protocols. Take the time to review your logs — you never know what you might uncover.

05 **BUILD A SECURITY TOOLKIT**
No single piece of software is going to handle all of your security needs. Be prepared for the unexpected by having the tools you need already in your arsenal.

06 **STAY INFORMED OF THE LATEST VULNERABILITIES THAT MAY AFFECT YOU**
The Internet is a wealth of information, use it to your advantage

07 **UNDERSTAND YOUR CLOUD SERVICE PROVIDERS SECURITY MODEL**
Security in the cloud is a shared responsibility. Get to know your provider, understand where the lines are drawn, and plan accordingly.

LEARN MORE ABOUT SECURING YOUR CLOUD INFRASTRUCTURE AT WWW.ALERTLOGIC.COM