Yes Dorothy, You Can Secure the Cloud.

Secure by design in a public cloud

Whoami

25+ years of Unix system engineering experience

15 years within the Government (10 US Navy, 3 DoD contractor, 2 GS)

Spent last 10 years working in the private sector: Banking, large managed service provider (Rackspace) and now in consulting.

Currently a Solutions Architect with Six Nines IT. http://www.sixninesit.com

Specialize in CI/CD automation, cloud orchestration and configuration management

So Why am I here ?

This is a very OPINIONATED talk on building secure clouds as well as lowering the overall cost of ownership of your systems and security overhead.

- Native tools that make your life easier in the clouds
- Reduce the cost by lowering the number of managed systems. Security is part of the system not an ADD-ON.
- Remove redundant monitoring and logging. Systems and Security teams should be using the same tools, security is no longer special with an unlimited budget.
- This talk uses AWS, but 99% of this applies to all major public clouds.

Various AWS Security Tools :

Key Management System - Service that creates and stores encryption keys

CloudHSM - Hardware Key Storage and Management System

Certificate Manager - SSL/TLS creation and storage tool

AWS Shield - DDoS protection

AWS WAF - Web Application Firewall

Various AWS Security Tools (Page 2)

Amazon Inspector - Security Assessment Tool

AWS Directory Services - Microsoft AD or LDAP'ish directory services tools

Identity and Access Management (IAM) - Control User access to AWS services

AWS Artifact - Compliance Artifact reports

Cloud Config - Keeping your systems within set standards

See more details https://aws.amazon.com/products/security/

Good Network Design
the ‘Original Fundamental’

Basic network design work is still IMPORTANT. In my experience this is the number one failure most organization make when going to the cloud.

- Don’t be shy about network segmentation
- Use properly configured security groups on all devices
- Flow logs - when you just have to see and measure it all
- Add network devices as control point for each segment - For the true control freaks

Encrypt All the Things
(Yes Really still talking about this is 2017)

- Virtual Machines at Rest - File system level or whole VM
- Encrypt the data even within services (such as RDS, Caching etc)
- In Transit encryption - SSL tunnel everything
- Don’t Forget your backups and object stores

Logging and Monitoring

All the major cloud provider have huge customizable built-in systems for monitoring and log analysis.

Most of these tools are free, the only charges are normally storage.

- Centralized real time log gathering and analysis
- Store everything forever at very low cost (fractions of a penny per GB using AWS Glacier service for example)

Example of how this all can work for you

Generate alerts based on SSH failures:

http://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudwatch-alarms-for-cloudtrail.html#cloudwatch-alarms-for-cloudtrail-authorization-failures

More Example Fun

Scripts to automate IAM password and key age usage.

Password key age - list all the keys that are older than X days

Password key last used - list all the keys that have not been utilized in X days

https://github.com/cybermerc/aws_audit_tools

Questions ?

Slides and Notes

https://github.com/cybermerc/bsidessanantonio_2017