Seven Secrets of
AWS Security

Executive Summary

Security is a pain in the ass.

It is that simple, and this is why so many computing systems are so vulnerable: people are lazy. There is a clear, inverse correlation between security and convenience – good security is truly a pain in the ass, and extremely expensive. Good security is expensive because people have to jump through so many additional hoops.

And good security needs excellent IT management, which is generally lacking. Far too often, IT "management" seems to consist almost entirely of attending the latest Gartner seminar to be willingly indoctrinated in the latest fad; "bi-modal" is the current fad-of-the-week.

A practical example from the real world: a few years ago when the Web was the Bright New Thing, lazy programming managers (who would never dream of reading their programmers' code), allowed even more lazy programmers to scrap the screen for a password and to plop it directly into a SQL query, allowing even the dullest hacker to simply add a second query to the string. Sad.

Like on-premises virtual machines before it, AWS is very much a two-edged sword. When adding a new server consisted of trucking in a 25-ton behemoth to a specially prepared computer room, planning was exhaustive and exhausting. Today, it is three minutes work from a mobile phone, and today's server is 100-fold more powerful than the ancient behemoth.

With this dangerous informality, all too often little or no thought is given to security – "Amazon will do it." Wrong. Dangerously, catastrophically wrong.

It is highly likely that most AWS EC2 implementations are far less secure than the on-premise ones they replace.

Want proof? A recent study found over 1,000 misconfigurations in EC2 instances per AWS account.

This Argent AWS White Paper provides a simple check list for AWS security. Like everything in life, nothing is free. It is the main responsibility of competent IT management to strike the appropriate balance with respect to convenience versus security.

Secret 1: Who's On First; No, Who's On Second

Geeks – and all-too-often, their managers – love new toys.

As AWS is the newest and brightest new toy, everyone wants a piece of the action. And now! In this haste, no proper management structure is created for the mushrooming AWS implementations, and this is especially true of the only really critical management role -- AWS Security Czar.

The best way of implementing this is to start by creating an AWS Security Department. Yes, a department through which all AWS implementations and security changes must pass. This team of security specialists has two goals: to vet ongoing changes and to constantly preach to all AWS admins the **dangers** of AWS.

Admins, like programmers, will cut corners when they know they can get away with it. The specialist AWS Security Department must be the stern mother, not the always-indulgent father. As AWS has an ever growing list of features, so security training must never end.

Secret 2: Logs

Far too many admins create EC2 Instances and fail to turn on all the logging. Sometimes this is sloth, but more often it is simple ignorance. This is especially true for neophyte AWSers who mistakenly believe just creating the EC2 Instance is sufficient.

But AWS CloudTrail is essential (and it's often useful for debugging as well). CloudTrail provides a chronological log of all AWS API calls, and records the identity of the caller, the caller's IP address, parameters and the values returned by the AWS service.

In a word, CloudTrail is gold-dust.

And the CloudTrail logs can be readily and automatically checked by a number of third-party products, such as Argent for Compliance.

In addition, CloudTrail logs can be boiled down to provide extremely effective trend analysis and capacity planning.

One of the odd quirks of CloudTrail is that it cannot be turned on retroactively – this is yet another reason for the creation of the AWS Security Department: to prevent these dangerous creation oversights.

Secret 3: Too Many With Unnecessary Privileges

Without a formal plan and catalog of who has what privileges and why, security rapidly collapses, and needlessly allocated elevated privileges are granted to far too many people.

Worse, there is never any review of why an admin has so many elevated privileges.

Worse still, there is often no automated daily report of newly departed employees that maps to their AWS rights and privileges. Countless studies have shown long-departed former employees still holding all the keys to the castle.

This is where the AWS Security Department described in Secret 1 is a lifesaver.

"External auditor" is often defined as "those obnoxious know-it-all outside accountants who come in and tell us everything we are doing is wrong." Good. In some cases the traditional outside auditors do find genuine errors; in all cases, the threat of periodic visits by the persnickety auditors keeps the in-house accounting staff on their toes.

The same goes for admins – the AWS Security Department needs to conduct quarterly security reviews of every admin with any access to AWS. Very effective and very much a pain in the ass – good security is not cheap.

And all security requests need to be vetted by the AWS Security Department; this is how the chronic problem of IT's laziness can be corrected once and for all.

Secret 4: Silos Or Death

Good security requires planning and following the rules. In the Battle of Jutland, the British lost *Queen Mary* and *Indefatigable*, both disintegrated after being hit by German shells because the most basic rule of Action Stations – all water-tight doors being dogged – was ignored. When the more-accurate German shells rained down on both ships the resultant flashes ignited the cordite in the magazines. Rules are there for a purpose.

The "water-tight doors" of AWS is silos.

Design multiple accounts and multiple Virtual Private Cloud (VPC) definitions -- isolate workloads and independent teams.

Of course, testing, development, and production must be in separate, hermetically-sealed silos.

Secret 5: No Encryption

This is a no-brainer.

All RDS (Relational Database Service) and EBS (Elastic Block Storage) must be encrypted.

There can be no debate; "it is part of our AWS standards" is the refrain that every admin must know by heart.

Secret 6: Passwords Are Too Convenient

A very good rule in all security designs is: Easy = Bad.

This is actually a corollary of the first line of this white paper.

Many large companies – prestigious companies – companies that should (and probably do) know better, rely solely on passwords.

AWS has a rich array of optional facilities, such as two-phase authentication and physical cards. Sadly, these are optional and the lazy approach is the good old password.

In five or ten years, just using passwords will be illegal; the EU has been moving in that direction since August 2015.

Two-phase authentication must be the standard; passwords alone will not suffice.

Of course this also addresses the madness of the "passwords" of ’12345', 'secret', 'none', etc.

Secret 7: Instantly Fire Any Admin Using 0.0.0.0./0

Napoleon said, "After I execute one of my generals, all the others fight much better."

The same goes for any admin who uses 0.0.0.0/0. Using 0.0.0.0/0 allows any machine anywhere – think Russia or China – the ability to access your AWS resources.

AWS Security Groups can be used as wrappers around and EC2 Instance to police both inbound and outbound traffic; use them. And make them stern and severe – if in doubt, No!

For all remote access, always use a Bastion Host to provide an added layer of security (A Bastion Host is an EC2 Instance that acts as a clearing house; see https://en.wikipedia.org/wiki/Bastion_host for a good introductory description.)

One excuse sometimes heard is the need to patch "on-the-fly." Patching on-the-fly is like repairing a plane's wing while the plan is flying. Don't. Rather create a new image and a new Instance and apply the patch to this new Instance.