

The background of the slide features a light blue sky with white clouds. Numerous white padlock icons of varying sizes are scattered across the scene. On the right side, a hand is holding a black smartphone. The phone's screen displays a blue interface with a white document icon and some text, suggesting a mobile application or document viewer.

Pragmatic Cloud Security

Rich Mogull, Analyst & CEO, Securosis, LLC
@rmogull

events.techtarget.com

This Old Process



- Assess
- Redesign
- Secure
- Inspect
- Profit!

Assess

How would we be harmed if the asset became public and widely distributed?

How would we be harmed if an employee of our cloud provider accessed the asset?

How would we be harmed if the process or function was manipulated by an outsider?

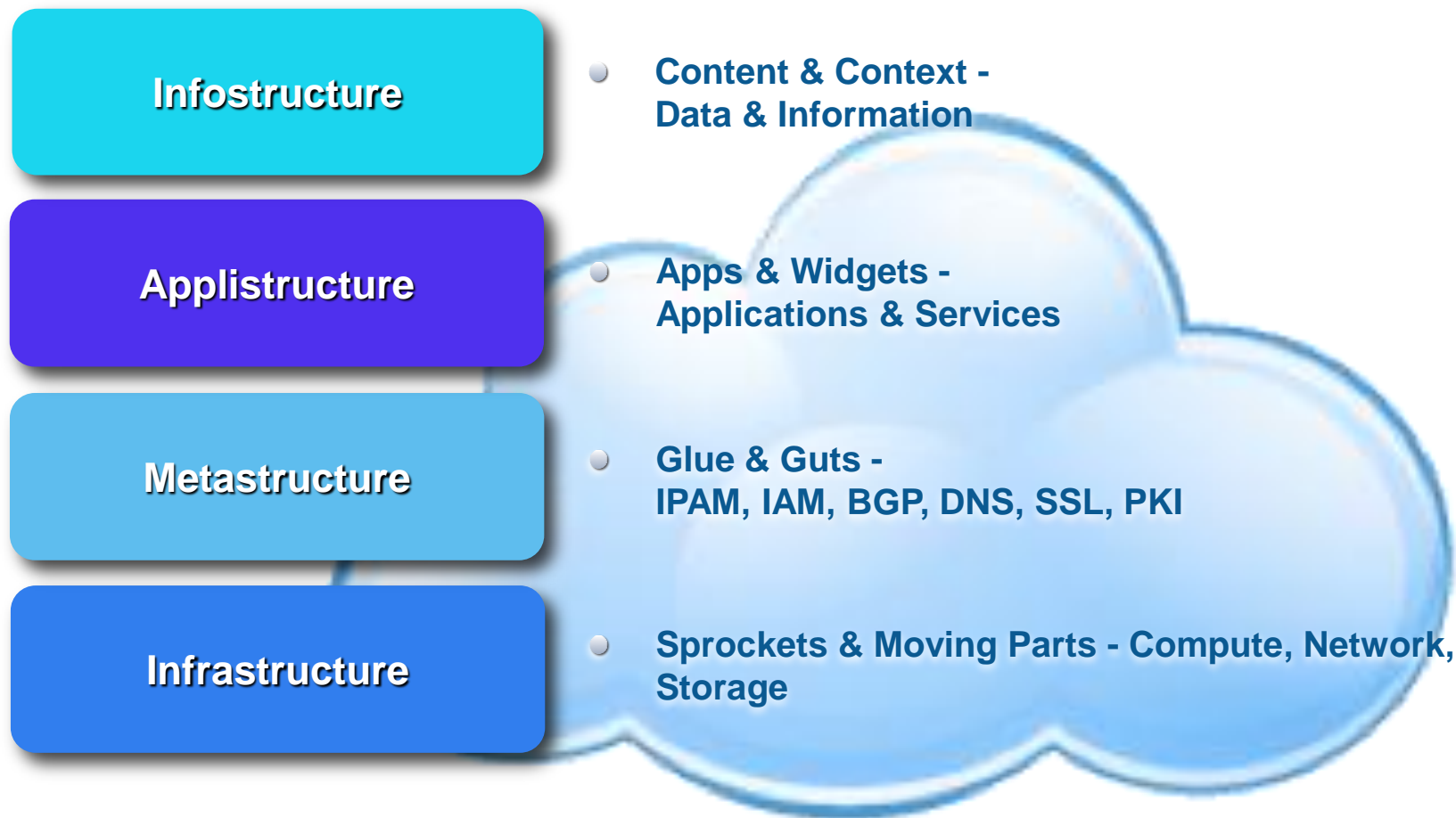
How would we be harmed if the process or function failed to provide expected results?

How would we be harmed if the information/data was unexpectedly changed?

How would we be harmed if the asset was unavailable for a period of time?

Can we maintain compliance when moving to the cloud?

The Stack



The Stack

Metastructure

- **Glue & Guts -**
IPAM, IAM, BGP, DNS, SSL, PKI

Secure Management Plane

Public

- * Admin IAM on roids
- * VPC Netsec
- * Automate management logging and alerting

Private

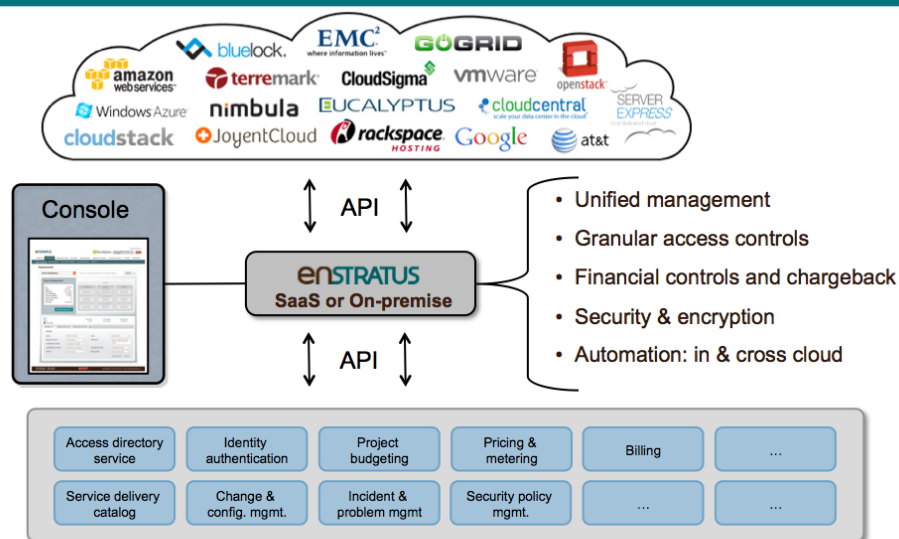
- * Upgrade all components
- * Config old-school netsec
- * Secure by architecture
- * Lock access
- * Mo Modular

Automate!

Metastructure Management



The Enterprise Cloud Management Solution



DIY Metastructure Mgmt

- API and CLI scripts
- Decent alerting, bad stopping



Automate Security

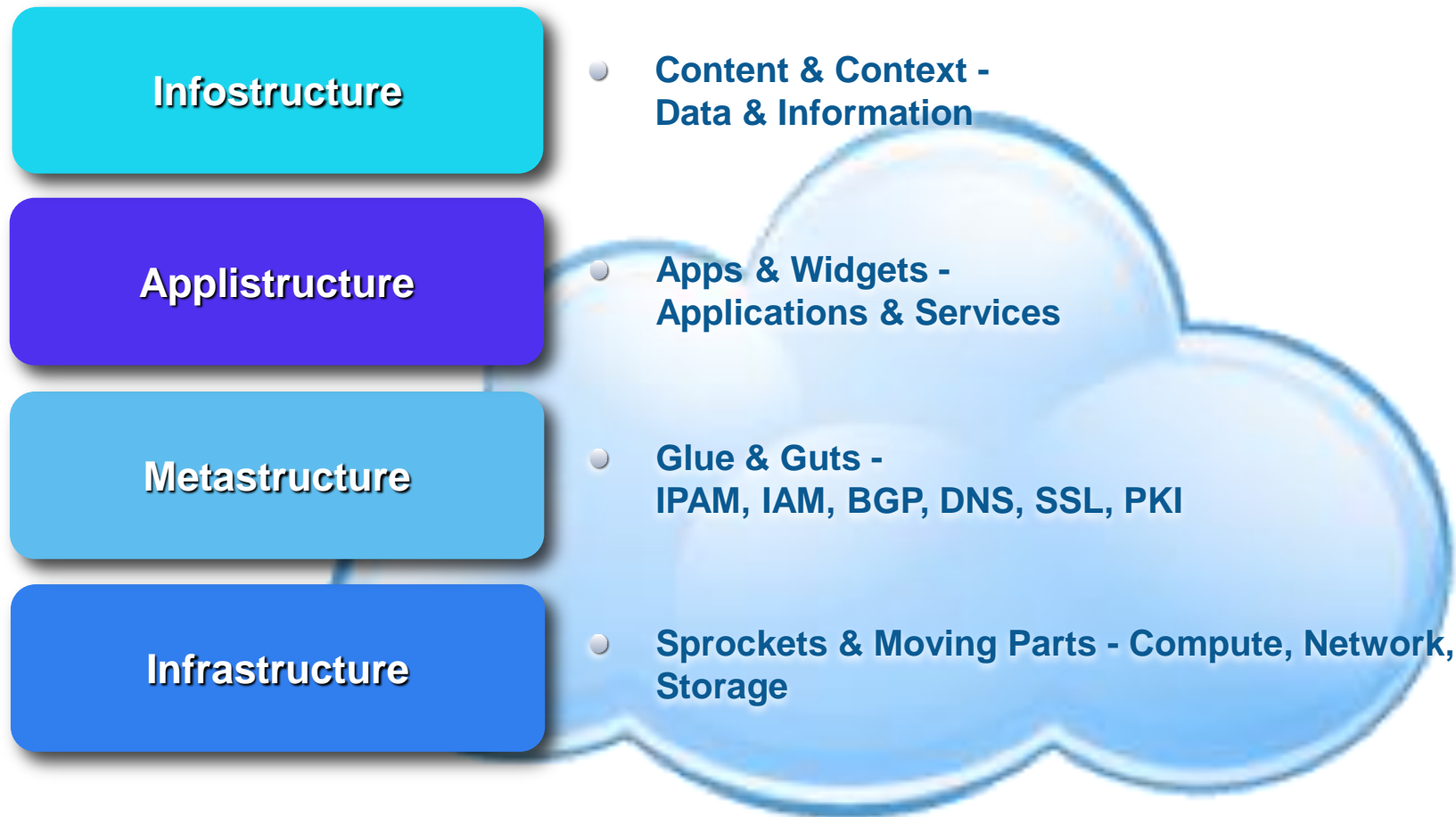


- E.g. Netflix Security Monkey
-

Review

- Lock down management plane
 - Focus on IAM for admins
 - Automate monitoring using cloud APIs
 - Look at metastructure management tools
-

The Stack

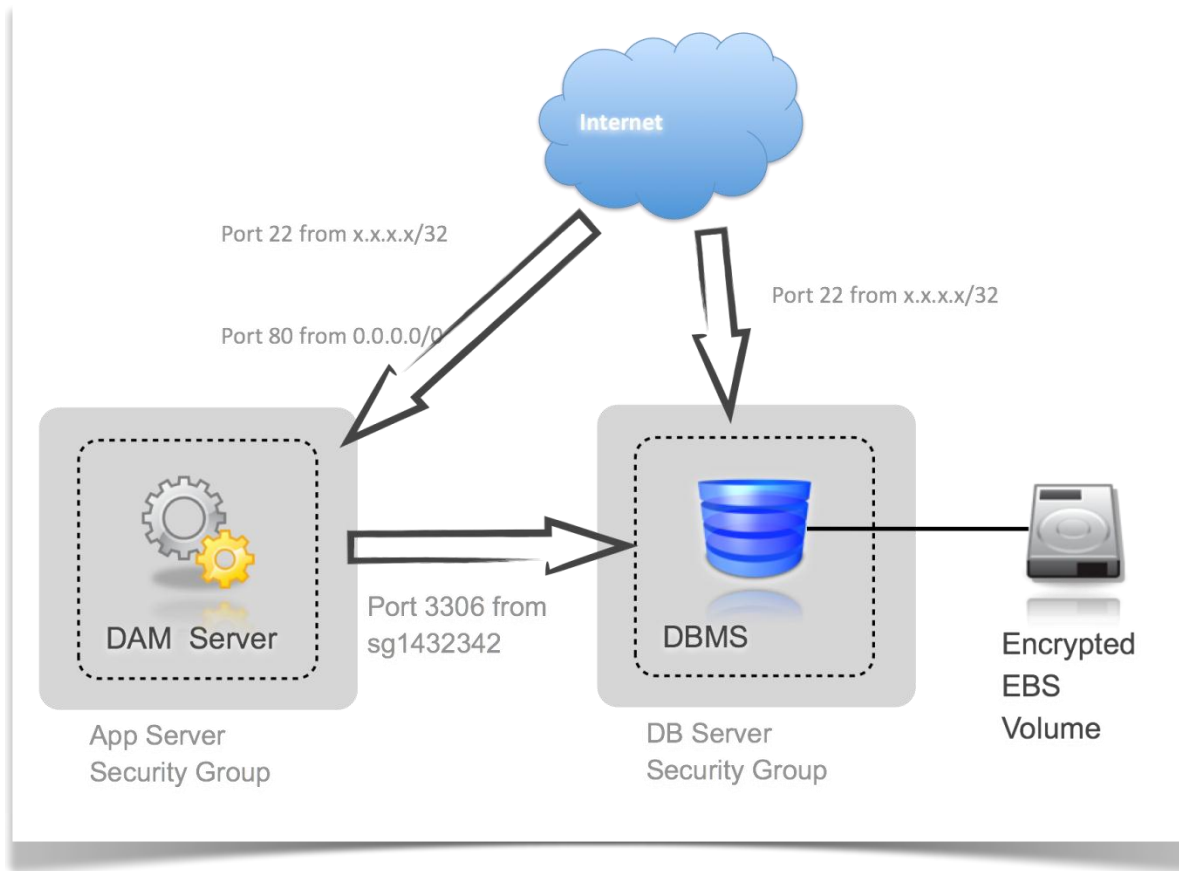


The Stack

Infrastructure

- **Sprockets & Moving Parts - Compute, Network, Storage**

Hypersegregate



**Dynamic, automatic, software defined
firewalls**

Host Automation



- Initialization scripts (cloud-init)
 - Install and config security agents
- Chef/Puppet
- Auto register and assess
- Privileged user mgmt and IAM

Demo



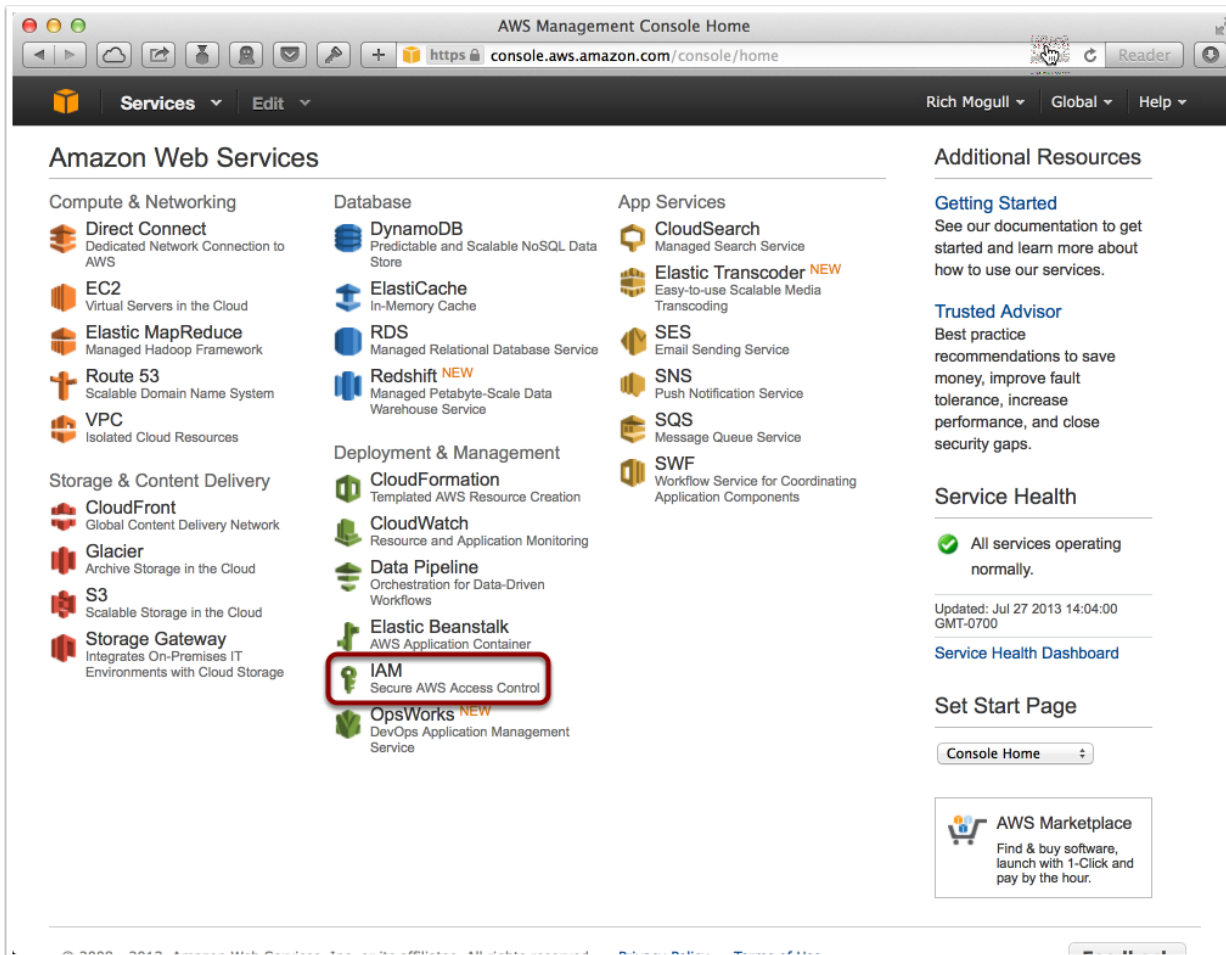
What We Will Do

- Automate cloud security policy compliance
 - Leverage S3, EC2, and APIs to bootstrap instance security polices.
 - Build a software defined security application
 - Glue multiple APIs together using Ruby to identify unmanaged instances.
-

Our Process

- Launch an instance
 - Assign an IAM Role
 - Use cloud-init to bootstrap Chef
 - Securely, and automatically, distribute security credentials
-

AWS IAM



IAM Management Console

https://console.aws.amazon.com/iam/home#home

Services Edit Rich Mogull Global Help

Dashboard


- Details
- Groups
- Users
- Roles
- Password Policy

Getting Started


AWS Identity and Access Management (IAM) enables you to manage access to your AWS resources.

[Create a New Group of Users](#)


What Are Users?

 Users interact with websites and services.


What Are Groups?

 Groups enable you to manage permissions for multiple users.



What Are Permissions?

 Permissions specify which actions a user can perform.

What Are Roles?




 Roles allow AWS services and IAM users to act on your behalf.

Security Status

- Root Account MFA  Disabled [Manage MFA Device](#)
- Password Policy  Disabled [Manage Password Policy](#)

IAM Resources

You are using the following IAM resources.

-  1 Group(s)
-  1 User(s)
-  1 Role(s)

AWS Account Alias

IAM Documentation

© 2008 - 2013, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#) [Feedback](#)

AWS IAM Roles

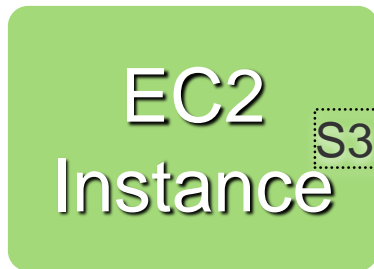
The screenshot shows the AWS IAM Management Console interface. The browser address bar displays the URL `https://console.aws.amazon.com/iam/home#roles`. The user is logged in as Rich Mogull. The left-hand navigation menu includes links for Dashboard, Details, Groups, Users, Roles (which is currently selected), and Password Policy. In the main content area, there is a blue button labeled "Create New Role" and a grey button labeled "Role Actions" with a dropdown arrow. Below these buttons is a "Viewing:" search bar. A table lists IAM roles with the following data:

Role Name	Creation Time
<input type="checkbox"/> ChefClient	2013-07-01 14:41 PDT

A red arrow points to the "Create New Role" button.

Using IAM Roles to Distribute Credentials

Role: ChefClient



S3 Tools



validator.pem
client.rb

Set Up Your S3 Bucket

The image illustrates the process of creating an S3 bucket in the AWS console through three overlapping screenshots:

- Top Screenshot:** Shows the AWS Services navigation pane. The 'S3' service is highlighted with a red box and a red arrow pointing to it.
- Middle Screenshot:** Shows the S3 console 'All Buckets' page. The 'Create Bucket' button is highlighted with a red arrow.
- Bottom Screenshot:** Shows the 'Create a Bucket - Select a Bucket Name and Region' dialog box. The 'Bucket Name' field contains 'security_creds' and the 'Region' is set to 'Oregon'. Below this, the 'Permissions' section is expanded, showing a grantee 'rmogull' with permissions for 'List', 'Upload/Delete', and 'View Permissions' checked. There are also options to 'Add more permissions', 'Add bucket policy', and 'Add CORS Configuration'. 'Save' and 'Cancel' buttons are at the bottom right.

Create an IAM Role

Create Role Cancel

Specify a role name. You cannot edit the role name after the role is created.

Role Name:

Maximum 64 characters. Use alphanumeric and '+,=,@-' characters

Progress: CONFIGURE ROLE | ESTABLISH TRUST | SET PERMISSIONS | REVIEW

Create Role Cancel

Progress: CONFIGURE ROLE | ESTABLISH TRUST | SET PERMISSIONS | REVIEW

Select Role Type

- AWS Service Roles**
 - Amazon EC2**
Allows EC2 instances to call AWS services on your behalf. Select
 - AWS CloudHSM**
Allows AWS CloudHSM to create a network interface on your behalf. Select
 - AWS Data Pipeline**
Allows Data Pipeline to call AWS Services on your behalf.
 - Amazon EC2 Role for Data Pipeline**
- Role for Cross-Account Access**
- Role for Web Identity Provider Access**

Create Role Cancel

Progress: CONFIGURE ROLE | ESTABLISH TRUST | SET PERMISSIONS | REVIEW

Set Permissions

Select a policy template, generate a policy, or create a custom policy. A policy is a document that formally states one or more permissions. You can edit the policy on the following screen, or at a later time using the user, group, or role detail pages.

- Select Policy Template**
 - Amazon S3 Full Access**
Provides full access to all buckets via the AWS Management Console. Select
 - Amazon S3 Read Only Access**
Provides read only access to all buckets via the AWS Management Console. Select
 - Amazon SES Full Access**
Profiles full access to Amazon SES via the AWS Management Console. Select
 - Amazon SES Read Only Access**
Select
- Policy Generator**
- Custom Policy**
- No Permissions**

Create Role

Cancel 

CONFIGURE ROLE

ESTABLISH TRUST

SET PERMISSIONS

REVIEW

Set Permissions

You can customize permissions by editing the following policy document. For more information about the access policy language, see [Overview of Policies](#) in Using IAM.

Policy Name

AmazonS3ReadOnlyAccess-Chef-201307271409

Policy Document

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Resource": "*"
    }
  ]
}
```

[Back](#)

Create Role

Cancel 

CONFIGURE ROLE

ESTABLISH TRUST

SET PERMISSIONS

REVIEW

Review the following role information. To edit the role, click an edit link, or click **Create Role** to finish.

Role Name Chef

[Edit Role Name](#)

Trusted Entities The service ec2.amazonaws.com

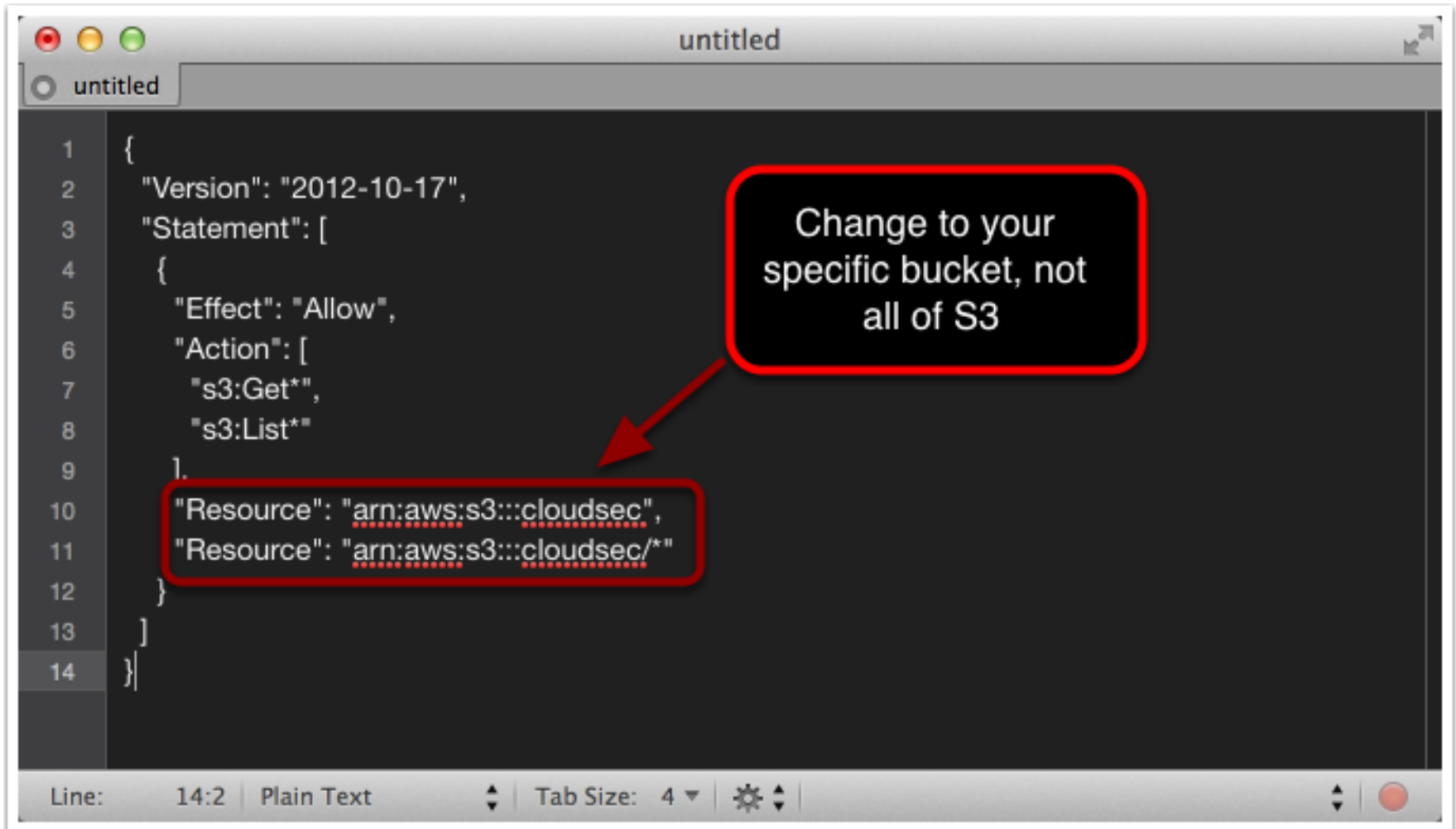
Permissions Amazon S3 Read Only Access

[Edit Permissions](#)

[Back](#)

Create Role

Adjust IAM Role Policy for Your Bucket



```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "s3:Get*",
8         "s3:List*"
9       ],
10      "Resource": "arn:aws:s3:::cloudsec",
11      "Resource": "arn:aws:s3:::cloudsec/*"
12    }
13  ]
14 }
```

Change to your specific bucket, not all of S3

Line: 14:2 | Plain Text | Tab Size: 4

Setting The Role of an EC2/VPC Instance

Request Instances Wizard

Cancel

CHOOSE AN AMI **INSTANCE DETAILS** CREATE KEY PAIR CONFIGURE FIREWALL REVIEW

Number of Instances: 1 **Availability Zone:** No Preference

Advanced Instance Options

Here you can choose a specific kernel or RAM disk to use with your instances. You can also choose to enable CloudWatch Detailed Monitoring or enter data that will be available from your instances once they launch.

Kernel ID: Loading... **RAM Disk ID:** Use Default

Monitoring: Enable CloudWatch detailed monitoring for this instance (additional charges will apply)

User Data:

as text as file

(Use shift+enter to insert a newline)

base64 encoded

Prevention against accidental termination.

Termination Protection:

IAM Role:

- None
- Chef
- ChefClient

Shutdown Behavior: Stop

Tenancy: Default

< Back Continue

Insert Script

Request Instances Wizard Cancel

CHOOSE AN AMI **INSTANCE DETAILS** CREATE KEY PAIR CONFIGURE FIREWALL REVIEW

Number of Instances: 1 **Availability Zone:** No Preference

Advanced Instance Options

Here you can choose a **kernel** or **RAM disk** to use for your instances. You can also choose to enable CloudWatch Detailed Monitoring or enter data that will be available from your instances when they launch.

Kernel ID: Use Default **RAM Disk ID:** Use Default

Monitoring: Enable CloudWatch detailed monitoring for this instance (additional charges will apply)

User Data:

as text
 as file

```
- [ sh, -c, *fix_routing_silliness ]  
- [ sh, -c, *configchef ]  
- touch /tmp/done
```

(Use shift+enter to insert a newline)

base64 encoded

Prevention against accidental termination.

Termination Protection:

IAM Role: ChefClient

Shutdown Behavior: Stop

Tenancy: Default

[< Back](#) [Continue >](#)

Select Chef Security Group

Choose one or more of your existing Security Groups

sg-1e3adb71 - CCSK-Chef-Server
sg-bf48aed0 - default
sg-cf32dfa0 - quick-start-1

(Selected groups: sg-1e3adb71)

What You Didn't See

- We have a pre-configured Chef server
 - Our Chef server is in an isolated security group
 - We created a security group to launch instances in so they can connect to our Chef server
 - We created our Chef credentials
-

Chef

- Ruby based configuration management
 - Commercial, hosted, or open source
 - <http://opscode.com/chef>
 - *Policies as code*
 - Cross-platform
-

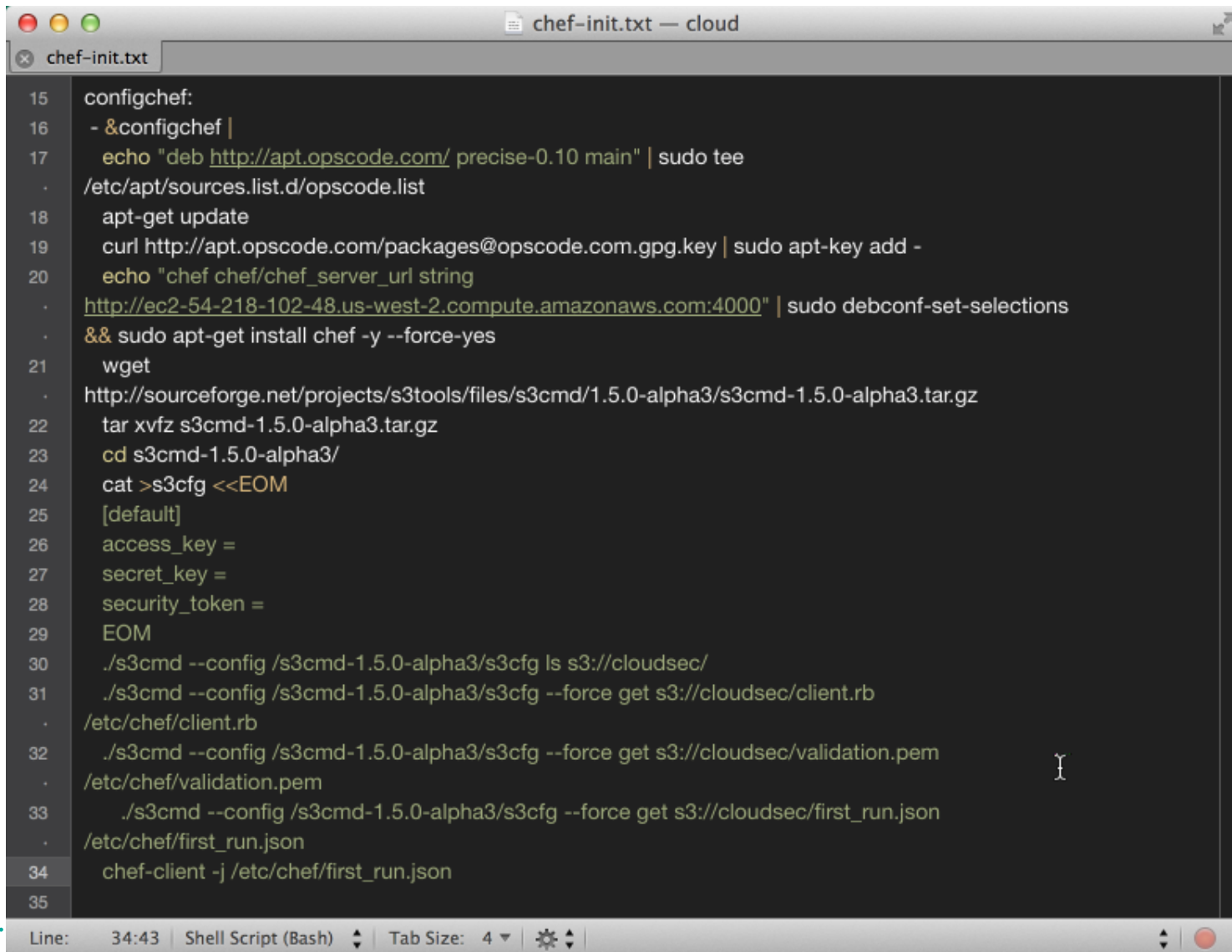
Chef Basics

- Server
 - Workstation
 - Node
 - Attributes
 - Recipe
 - Cookbook
 - Chef-repo
 - Environment
 - Knife
-

Chef Security

- Temporal certificate used for initial bootstrapping
 - Client certificate then issued
 - Per-node certificates
 - Per-client certificates
 - Organizations
 - Client IAM
-

Our Script

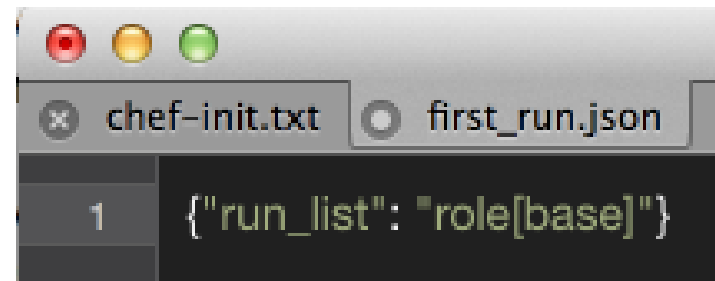


```
chef-init.txt — cloud
chef-init.txt
15 configchef:
16 - &configchef |
17   echo "deb http://apt.opscode.com/ precise-0.10 main" | sudo tee
   /etc/apt/sources.list.d/opscode.list
18   apt-get update
19   curl http://apt.opscode.com/packages@opscode.com.gpg.key | sudo apt-key add -
20   echo "chef chef/chef_server_url string
   http://ec2-54-218-102-48.us-west-2.compute.amazonaws.com:4000" | sudo debconf-set-selections
   && sudo apt-get install chef -y --force-yes
21   wget
   http://sourceforge.net/projects/s3tools/files/s3cmd/1.5.0-alpha3/s3cmd-1.5.0-alpha3.tar.gz
22   tar xvfz s3cmd-1.5.0-alpha3.tar.gz
23   cd s3cmd-1.5.0-alpha3/
24   cat >s3cfg <<EOM
25   [default]
26   access_key =
27   secret_key =
28   security_token =
29   EOM
30   ./s3cmd --config /s3cmd-1.5.0-alpha3/s3cfg ls s3://cloudsec/
31   ./s3cmd --config /s3cmd-1.5.0-alpha3/s3cfg --force get s3://cloudsec/client.rb
   /etc/chef/client.rb
32   ./s3cmd --config /s3cmd-1.5.0-alpha3/s3cfg --force get s3://cloudsec/validation.pem
   /etc/chef/validation.pem
33   ./s3cmd --config /s3cmd-1.5.0-alpha3/s3cfg --force get s3://cloudsec/first_run.json
   /etc/chef/first_run.json
34   chef-client -j /etc/chef/first_run.json
35
```

Line: 34:43 | Shell Script (Bash) | Tab Size: 4

Pre-assigning an IAM Role

```
. /etc/chef/client.rb
32 ./s3cmd --config /s3cmd-1.5.0-alpha3/s3cfg --force get s3://cloudsec/validation.pem
. /etc/chef/validation.pem
33 ./s3cmd --config /s3cmd-1.5.0-alpha3/s3cfg --force get s3://cloudsec/first_run.json
. /etc/chef/first_run.json
34 chef-client -j /etc/chef/first_run.json
```



A screenshot of a terminal window with a title bar containing three colored buttons (red, yellow, green) and two tabs: 'chef-init.txt' and 'first_run.json'. The 'first_run.json' tab is active. The terminal content shows a single line of JSON: `1 {"run_list": "role[base]"}`.

Role Run List

- Role: base
 - Cookbook: chef-client
 - Cookbook: delete-validator
-

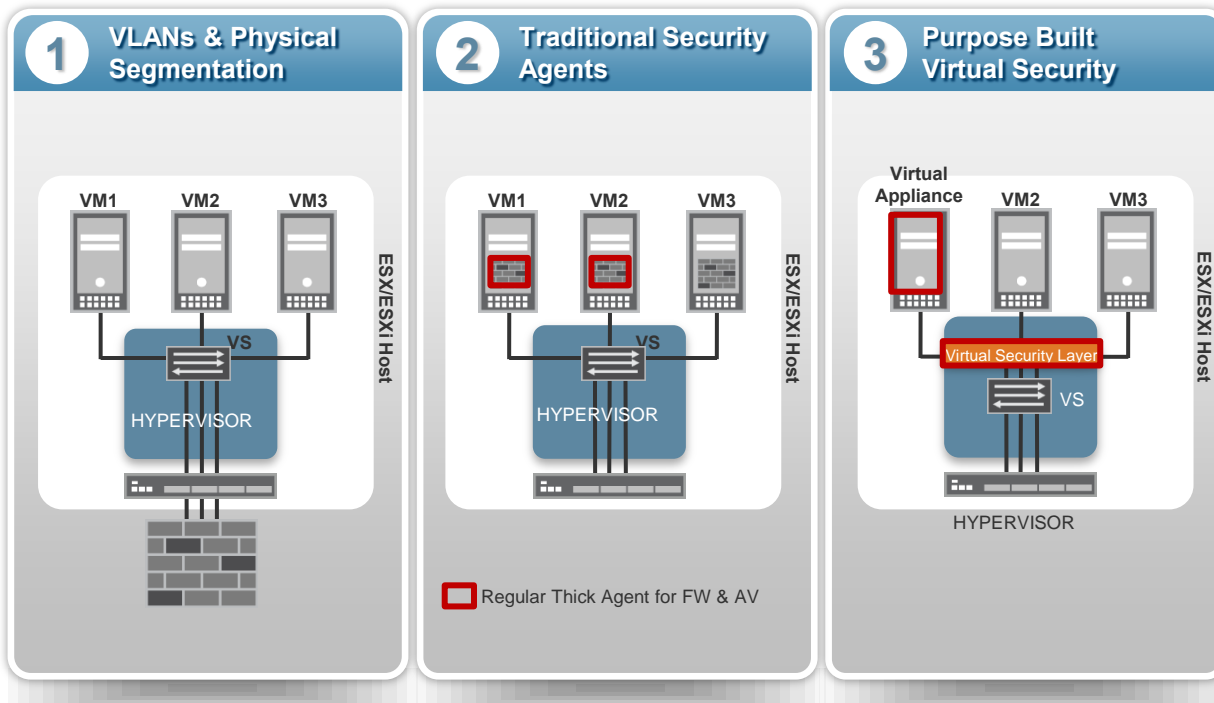


What is Happening

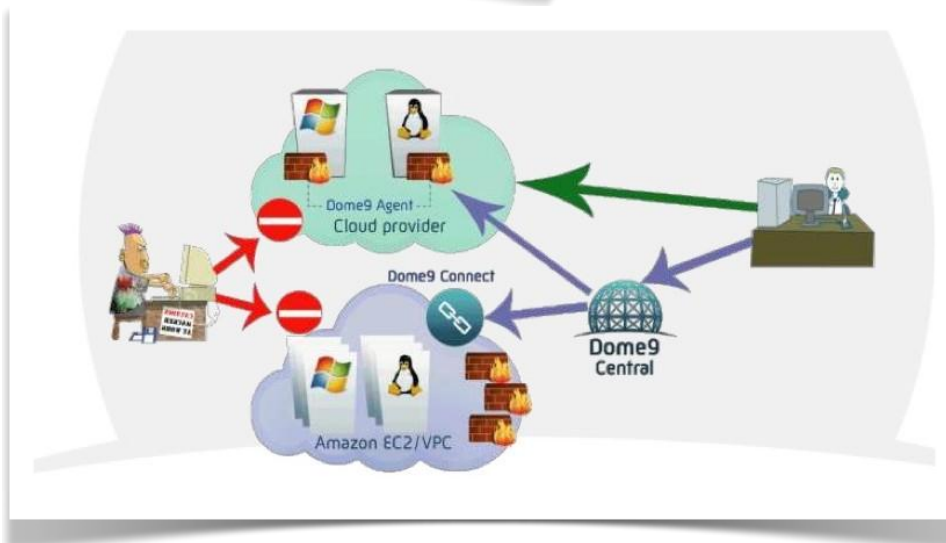
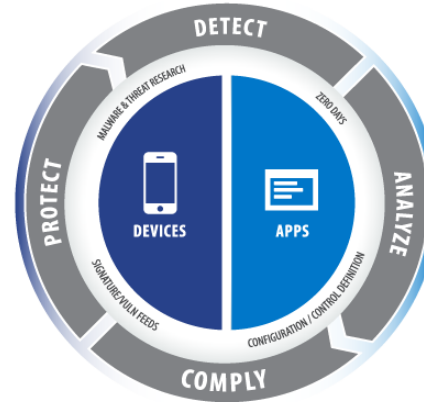
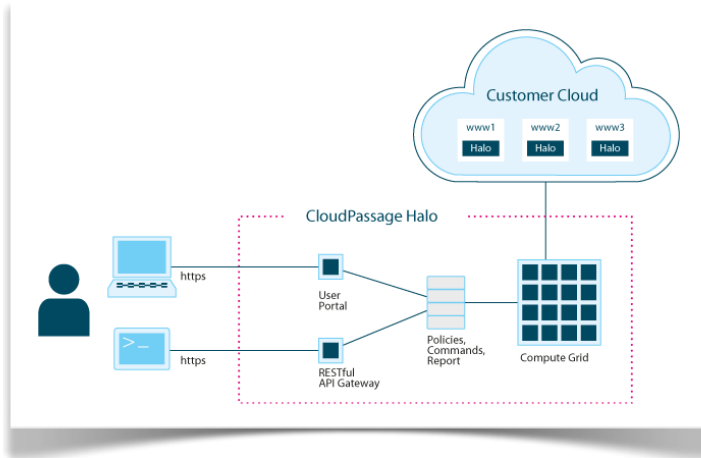
Review

- Security credentials stored securely in S3
 - Initialization script
 - Installs Chef
 - Downloads temp credentials *using* temp credentials
 - Configures Chef with initial role
 - Chef then pushes initial security policies
-

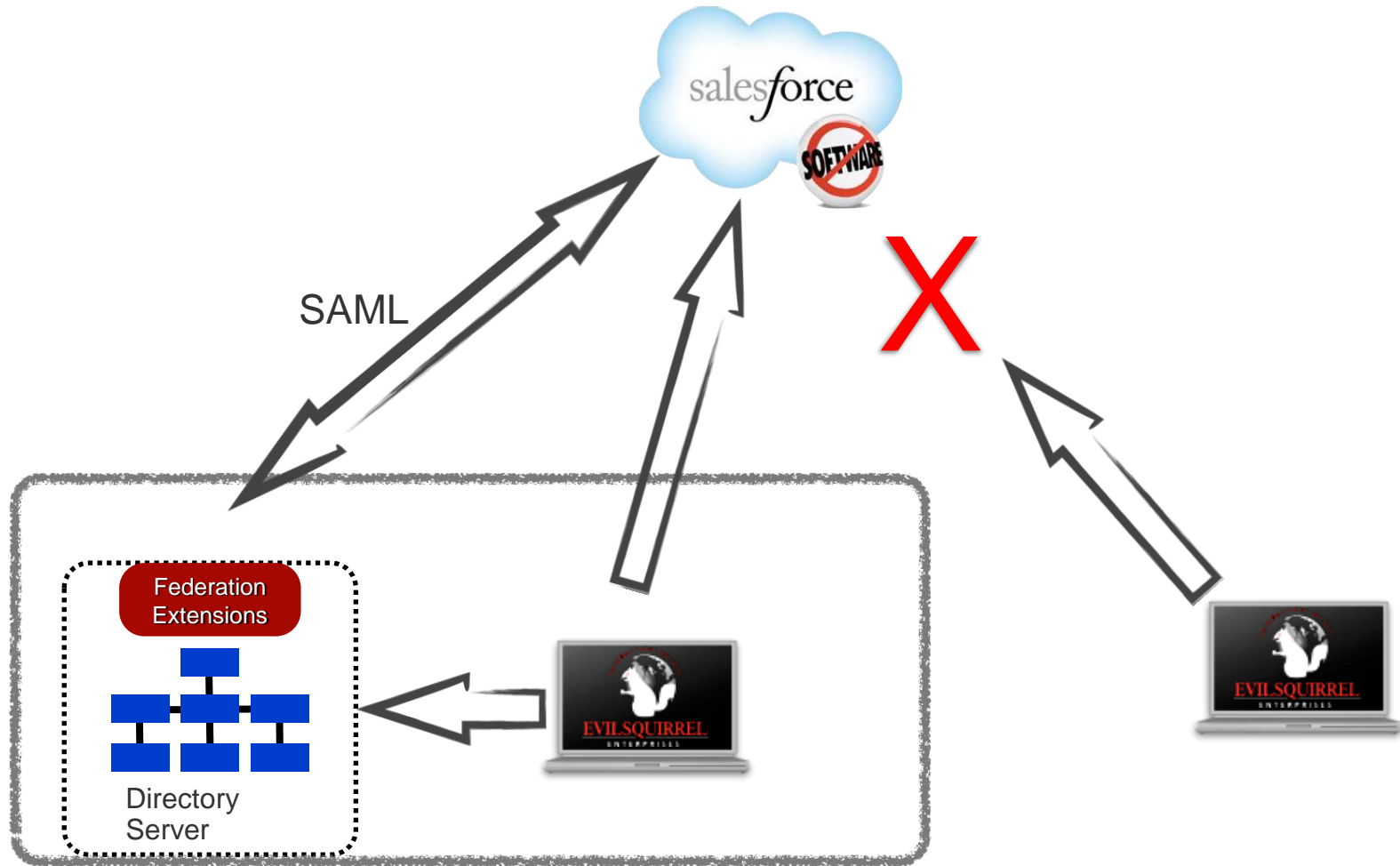
...Virtual Security Appliances & Introspection Solutions



Security & Compliance Platforms



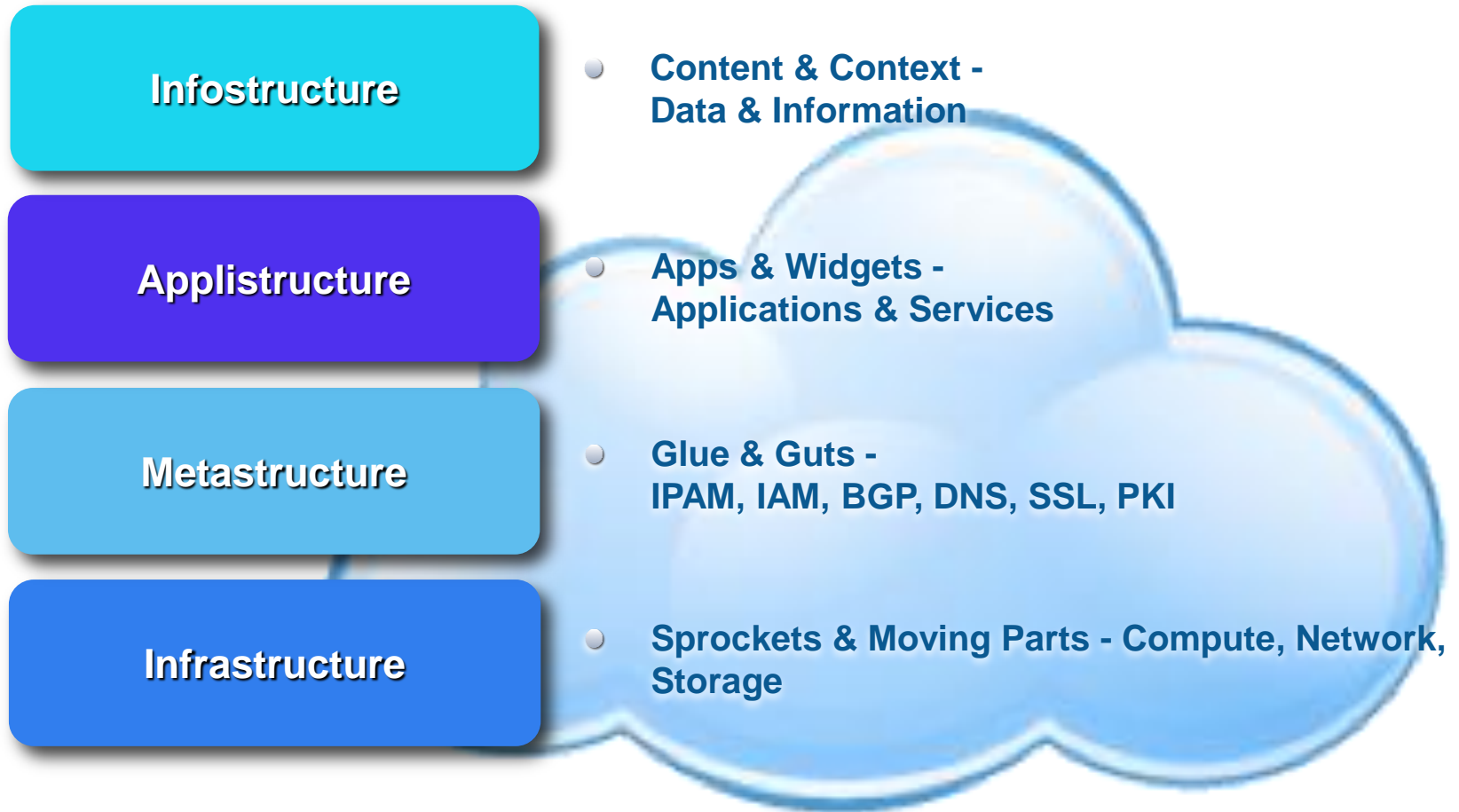
Restricting Device/Location with SAML



Review

- Hypersegregate- virtual, API-managed networks are your friends
 - Automate host security- from instance launch to assessment to patching
 - You will need tools to scale, even if you write them yourself
-

The Stack



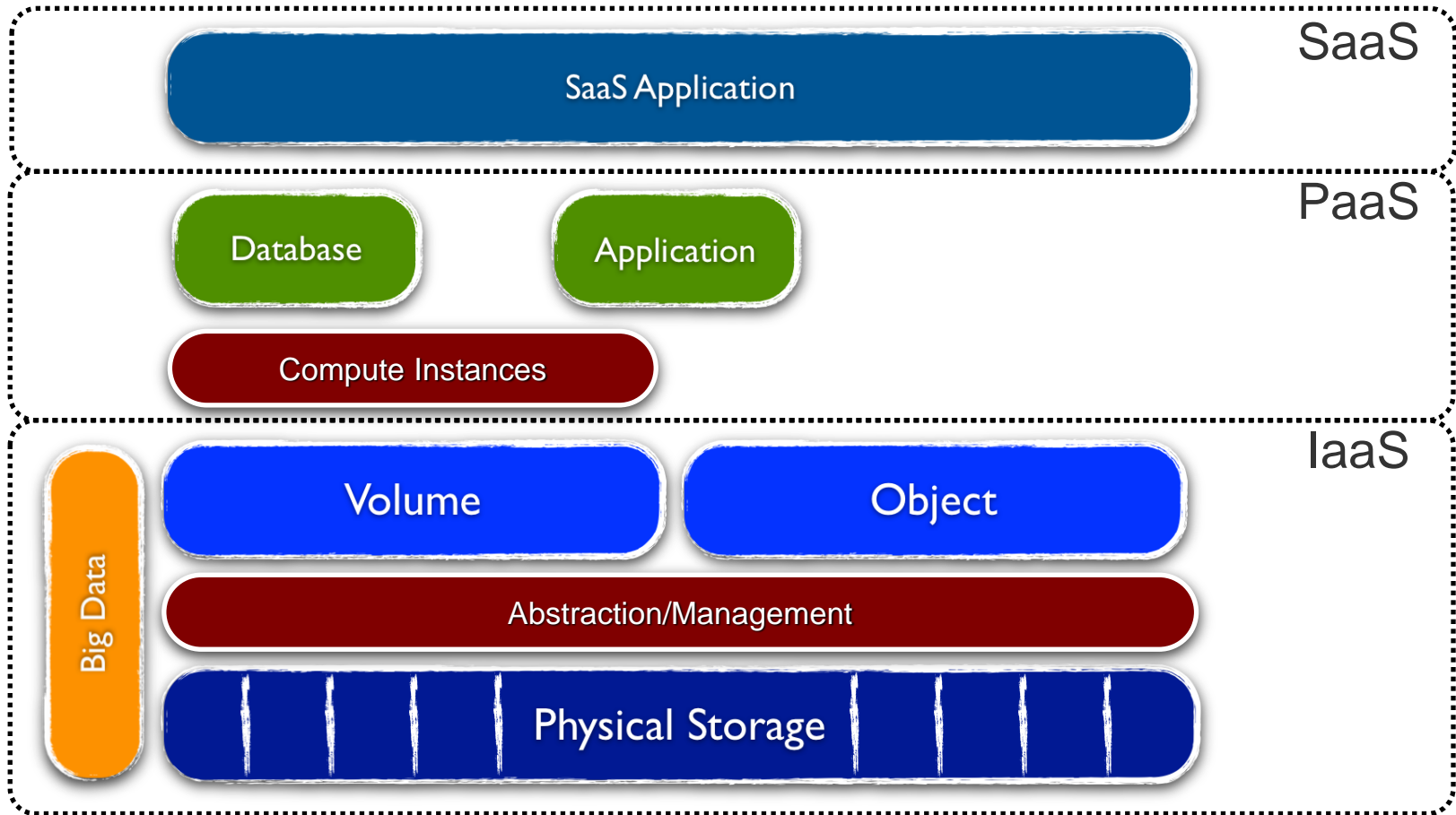
The Stack

Infostructure

- **Content & Context -
Data & Information**

Developed by Chris Hoff, Juniper

Cloud Data Architectures



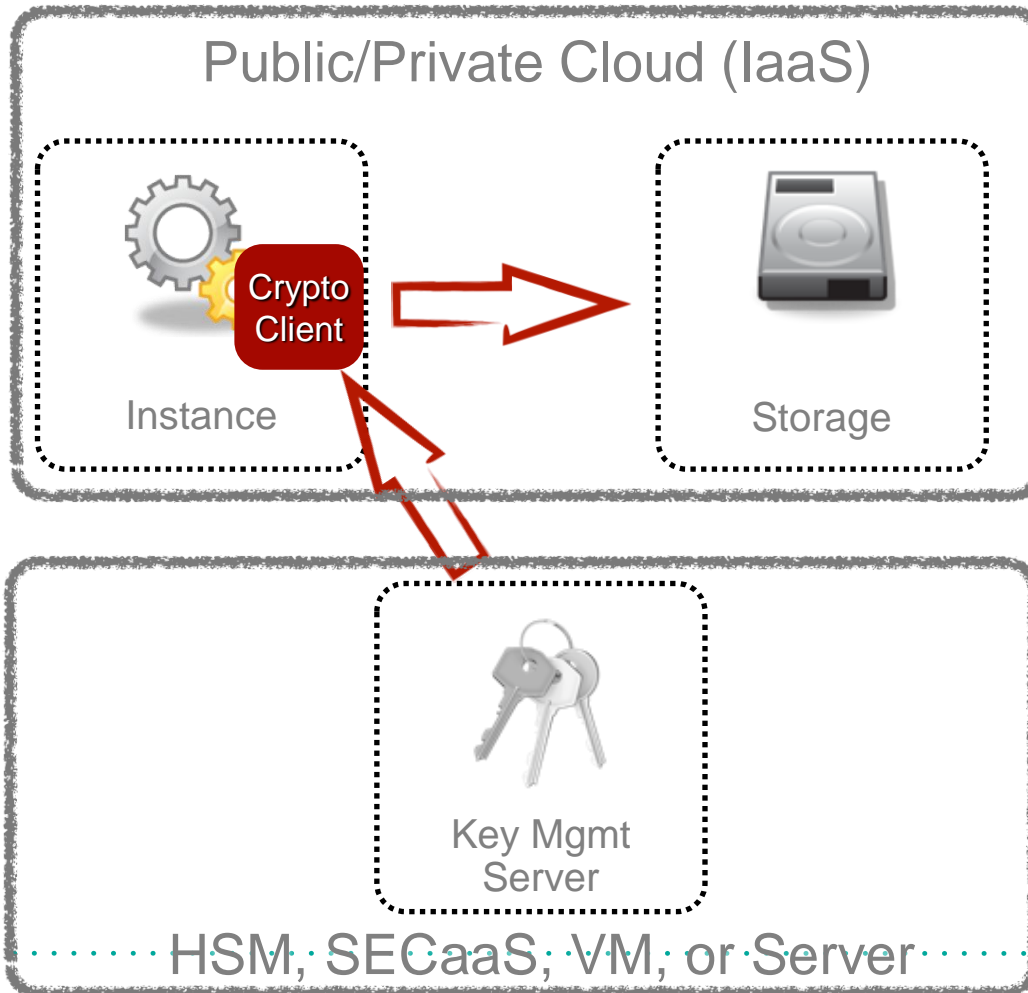
Keep Instances Clean

- Snapshots are not your friend.
- tmp, swap, keys



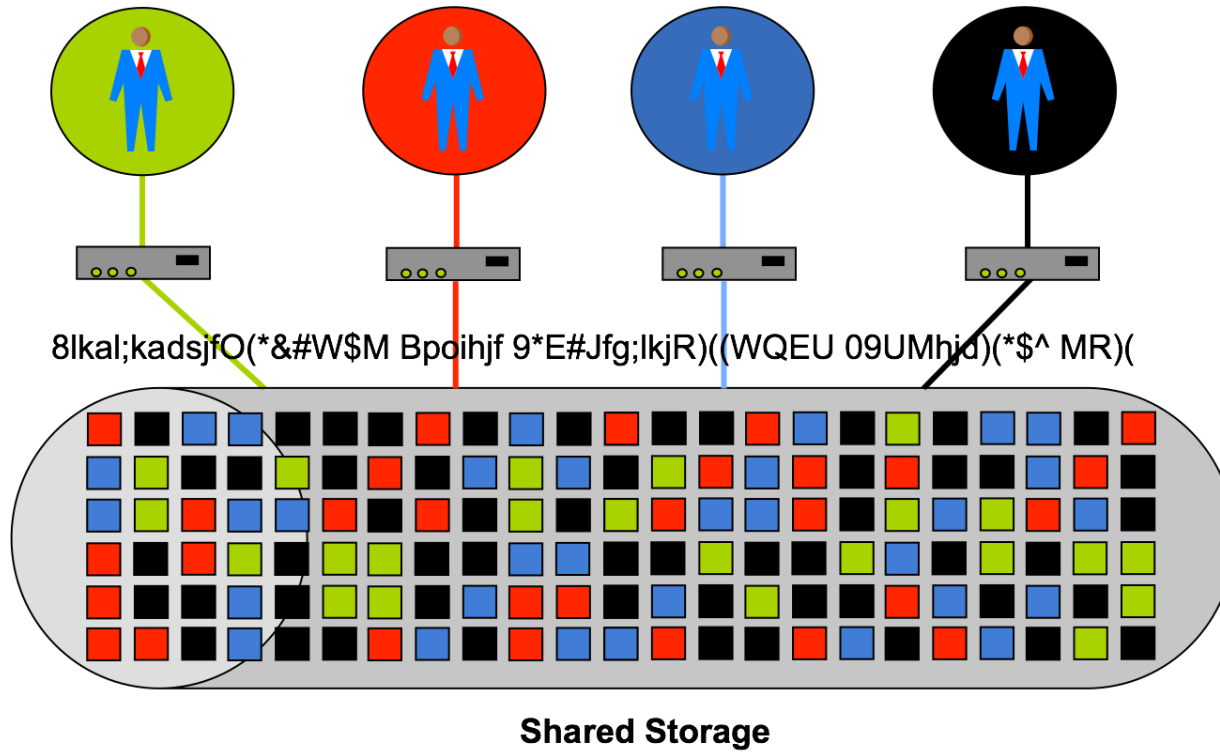
Volume Encryption

Protecting your snapshots since '09!



Object Storage Encryption

Or “how to use Dropbox without pissing off users *too* badly”



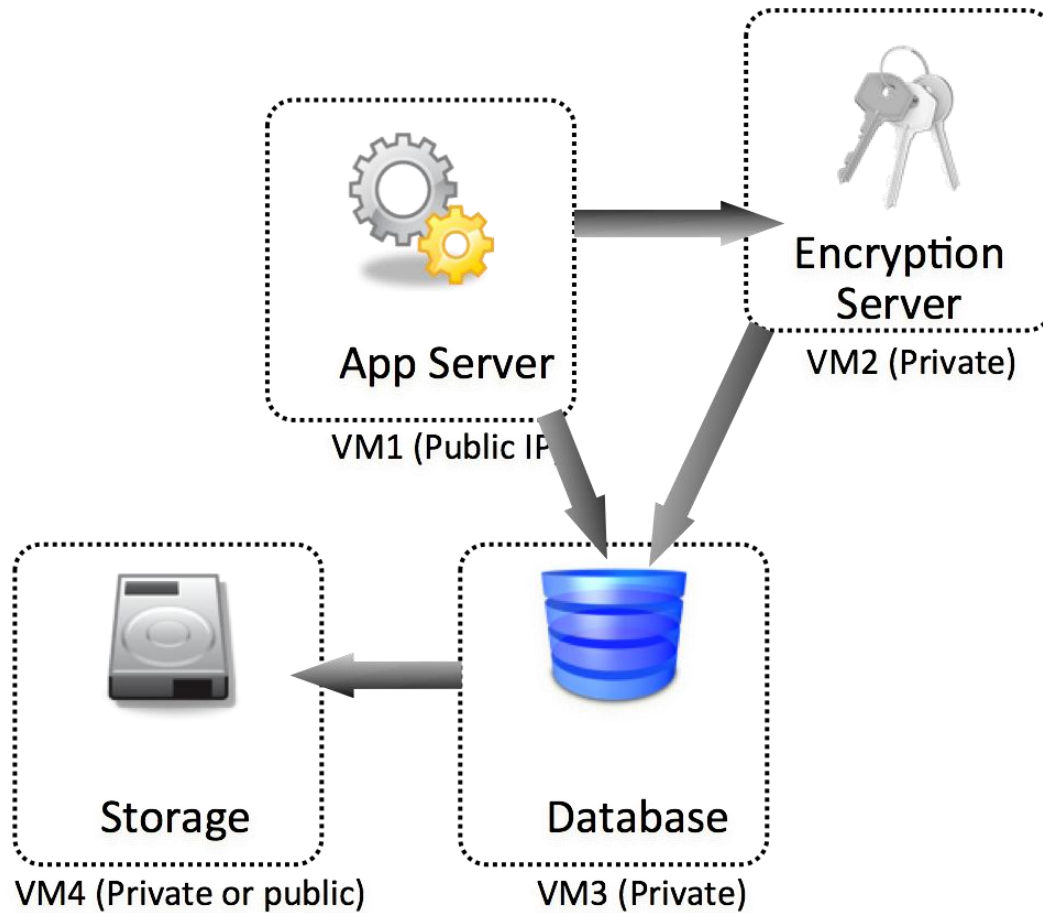
DB Security 4 Cloud

Table Security, get it?

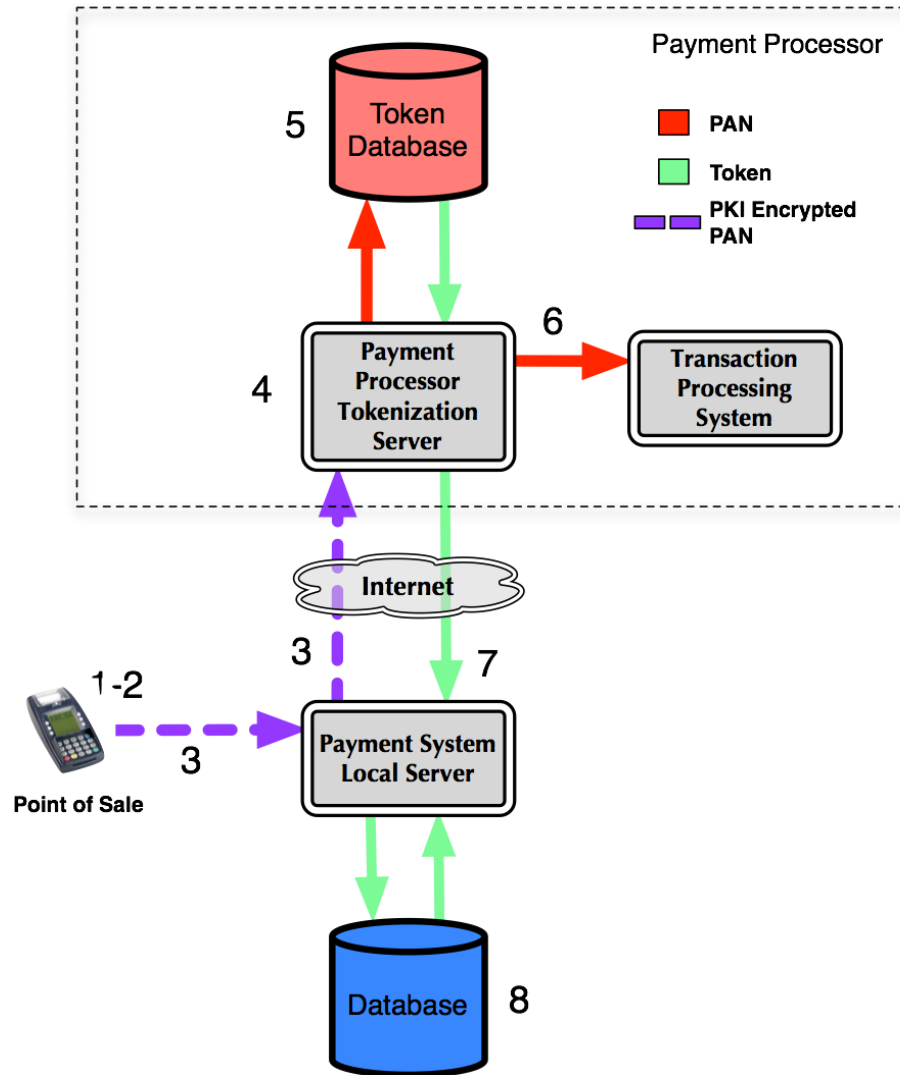


- Leverage architecture- segregate and split
- Use table views with CID, not direct table access
- Database Activity Monitoring
- Encryption

Cloud App Encryption



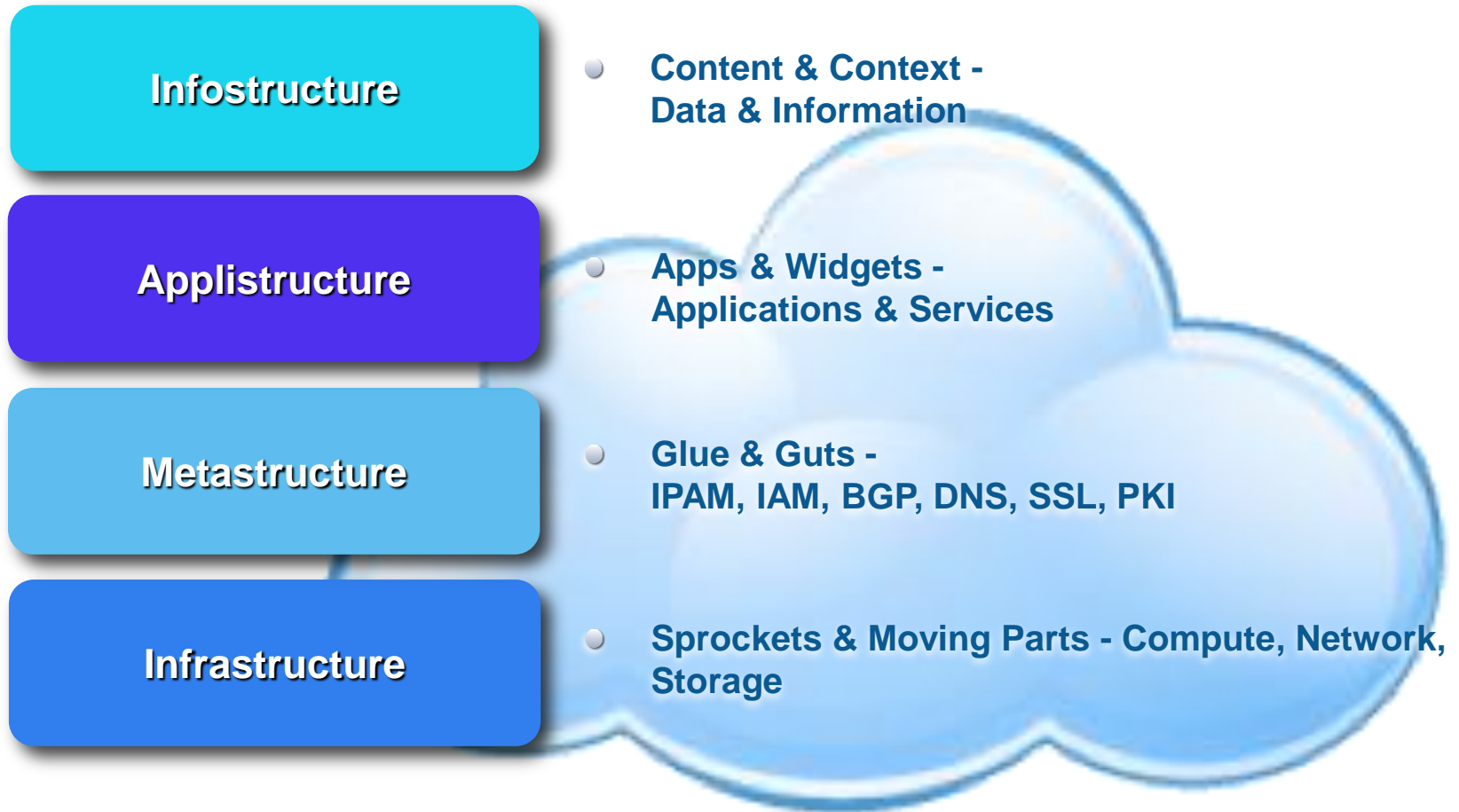
SaaS Tokenization



Review

- Keep your instances clean.
 - Encrypt volumes and don't store sensitive data in boot volumes.
 - Encrypt object storage data before it hits the cloud.
 - Follow good DB segregation.
 - Tokenize and/or encrypt data at the application layer when you can.
-

The Stack

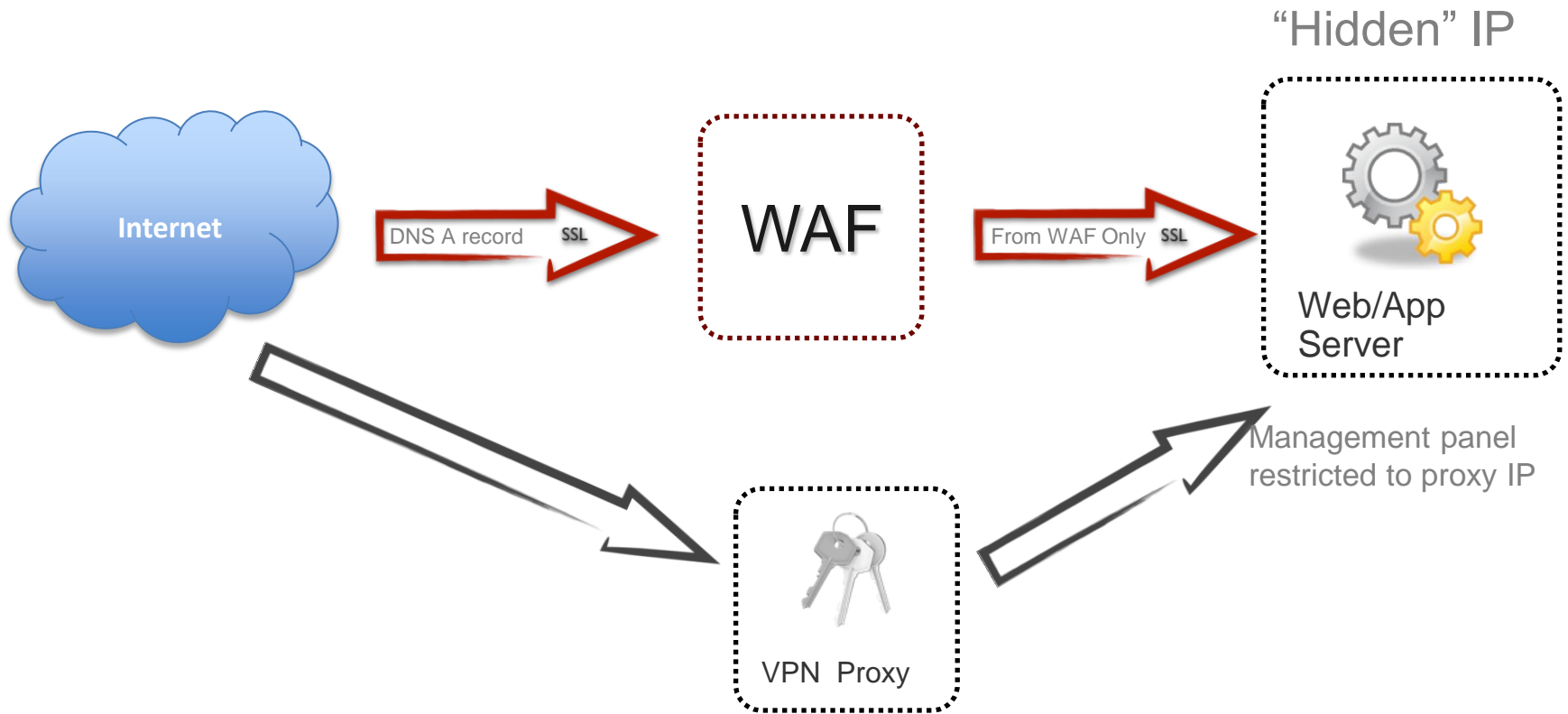


The Stack

Applistructure

- **Apps & Widgets - Applications & Services**

Cloud WAF



Test and Assess

- Test in private cloud or locked off network zone.
- DAST and web app vuln testing most useful.



Active Defense



Review

- Remember- at this point you are relying heavily on your secure foundation.
 - DAST and web app vulnerability testing are most useful.
 - Cloud WAF.
 - Mess with attackers using active defense.
 - Don't forget federated identity.
-

This Old Cloud

- Keep it simple
- Architect for cloud
- Split and encrypt
- Federate for success



Thank You!

- Rich Mogull
- Analyst/CEO
- nexus.securosis.com
- rmogull@securosis.com
- @rmogull

