Grilling Cloudicorns

Mythical CloudSec Tech You Can Consume Today

Christofer Hoff / Rich Mogull

Juniper Networks / Securosis

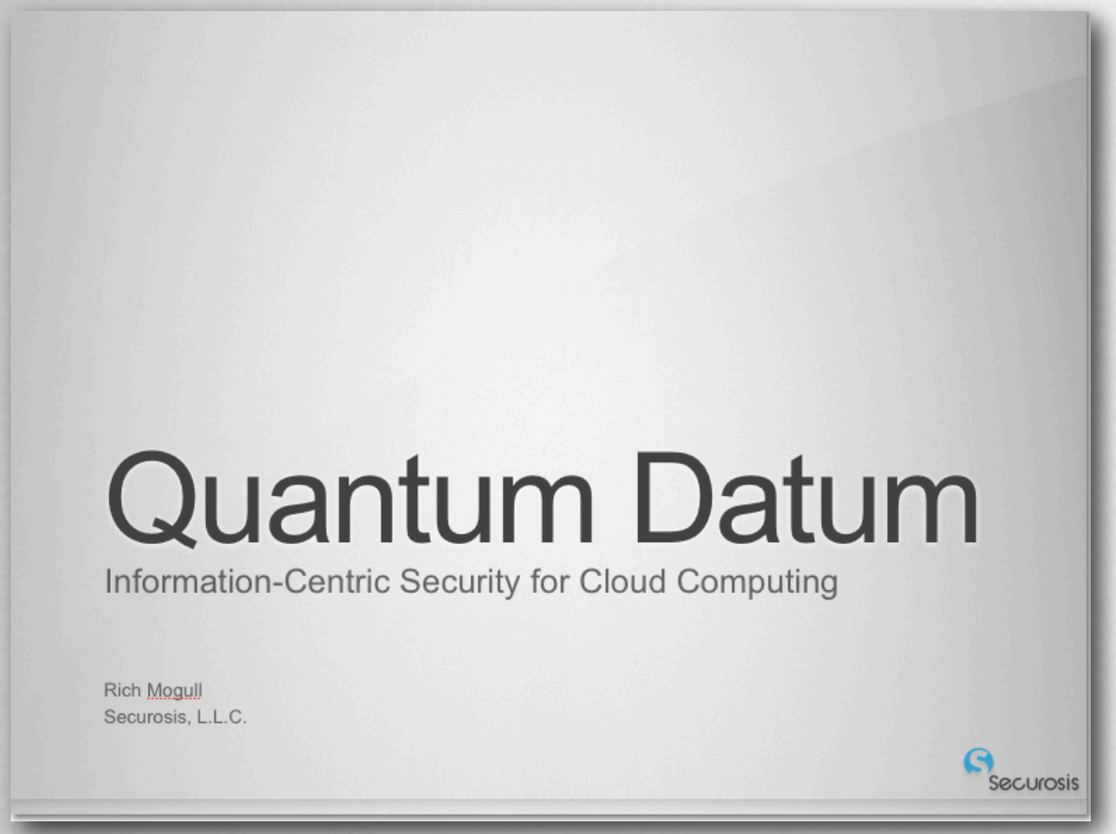
Session ID: EXP-304

Session Classification: Advanced

RSA CONFERENCE 2012

Agenda

- The Problem With Clouds
- The So-Called Dearth Of Cloud Security Solutions
- Solutions You Can Use Today



+

=

CloudiQuantaNomiDatumcon!

The Punchline

+ In The Simplest Of Terms, Using Cloud May Mean Imagining Applications & Information Across All “Tiers” Have The Potential To Be Connected Directly To The Internet...

+ We Often Can’t Trust The Provider, So We Must Engineer Security Into Design Patterns Across The Entire Stack

+ Any “Dumb” Component In The Stack Compromises The Integrity Of the Entire Stack...

+ APIs, Intelligence and Automation EVERYWHERE

The Future Of Security

- Content analysis fully integrated into both productivity and transaction applications.
- Rights (and thus encryption) applied at the point of creation, at the data-element level.
- Choke points between on-premise, off-premise, and between cloud services enforce policies at the data level, enforced by encryption/DRM.
- Policies and rights transfer and are maintained between state, phase and platform changes.

Photo by Caneles - http://flic.kr/p/4SGcdj

Securosis

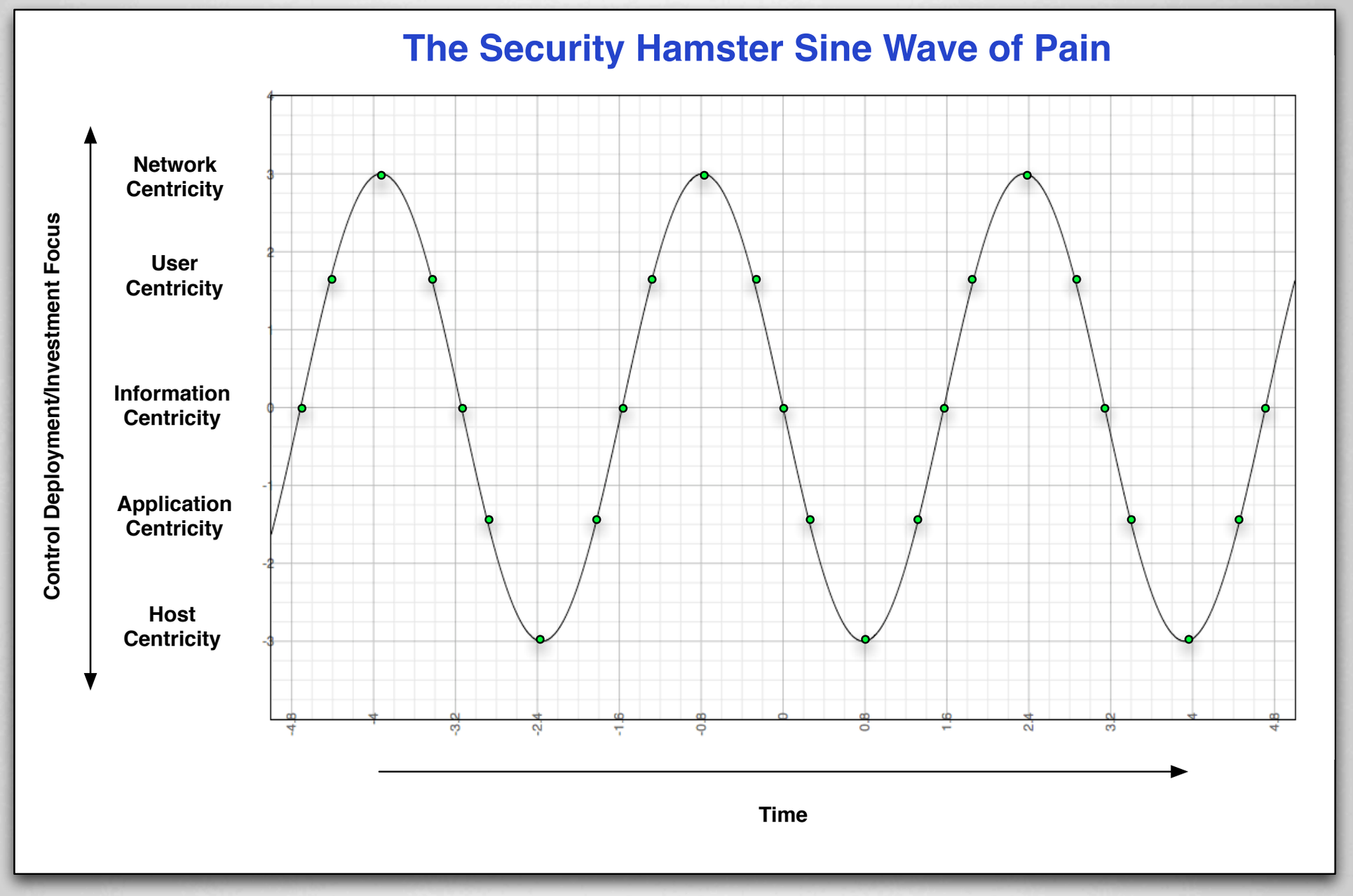
WINnovate

The Problem With Clouds

- Delivery/Deployment Model Differences with a horribly-abused Conflation of terms
- Should have been focusing on Apps/ Information in the first place
- Mobility and consumption models highlight huge security gaps when paired with cloud
- Emergence of network programmability, network virtualization, SDN and APIs
- The operational models and deployment options cause friction with design patterns of today

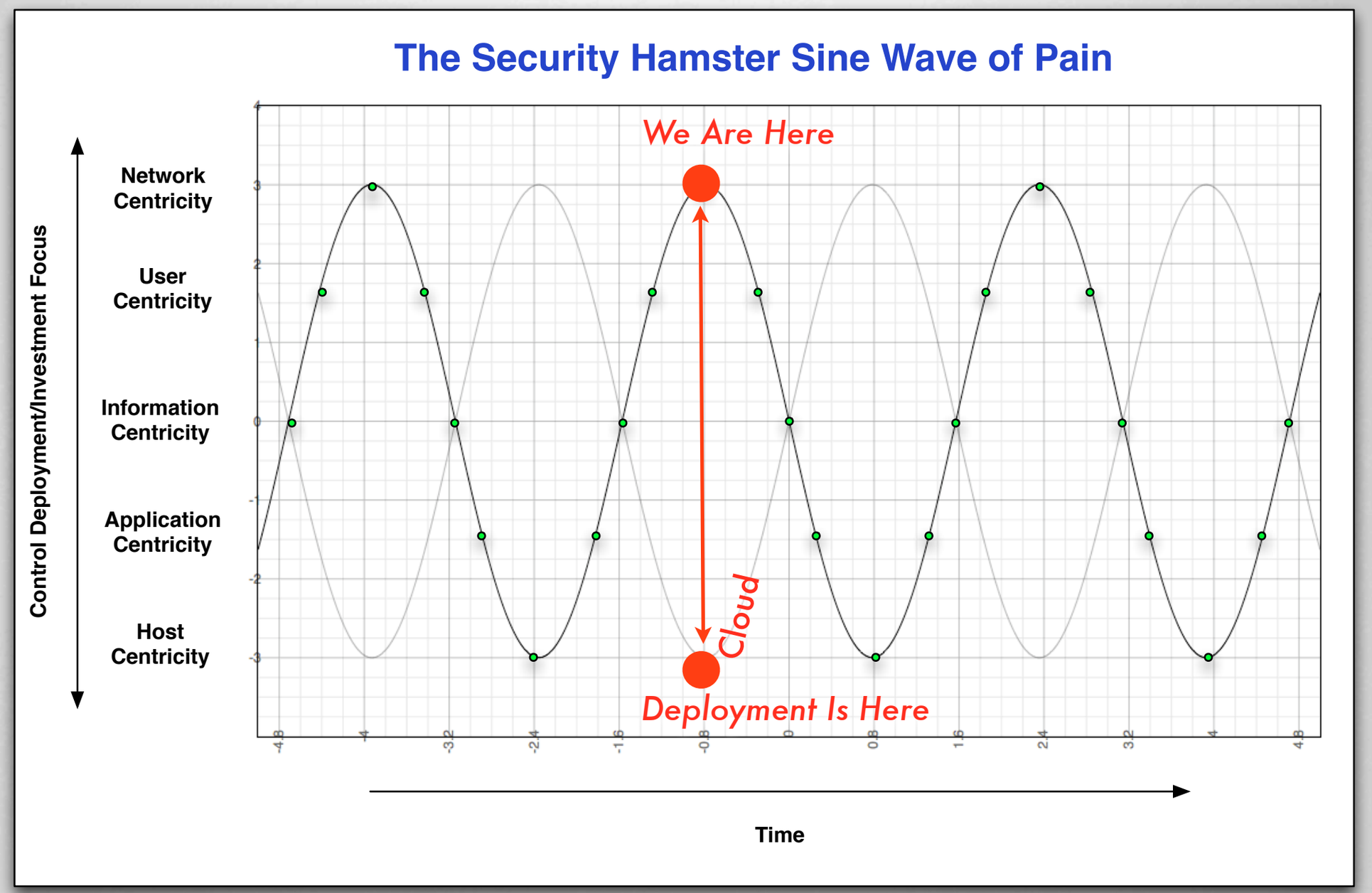
The So-Called Dearth Of Cloud Security Solutions

The Hamster Sine Wave of Pain...*



** With Apologies to Andy Jaquith & His Hamster...*

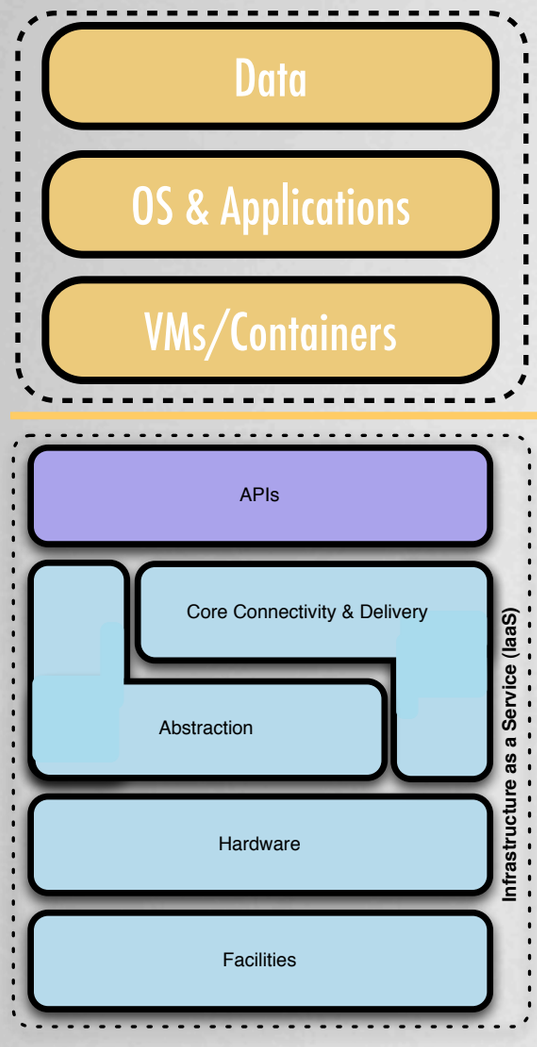
The Hamster Sine Wave of Pain...*



* With Apologies to Andy Jaquith & His Hamster...

How We Think About Security:

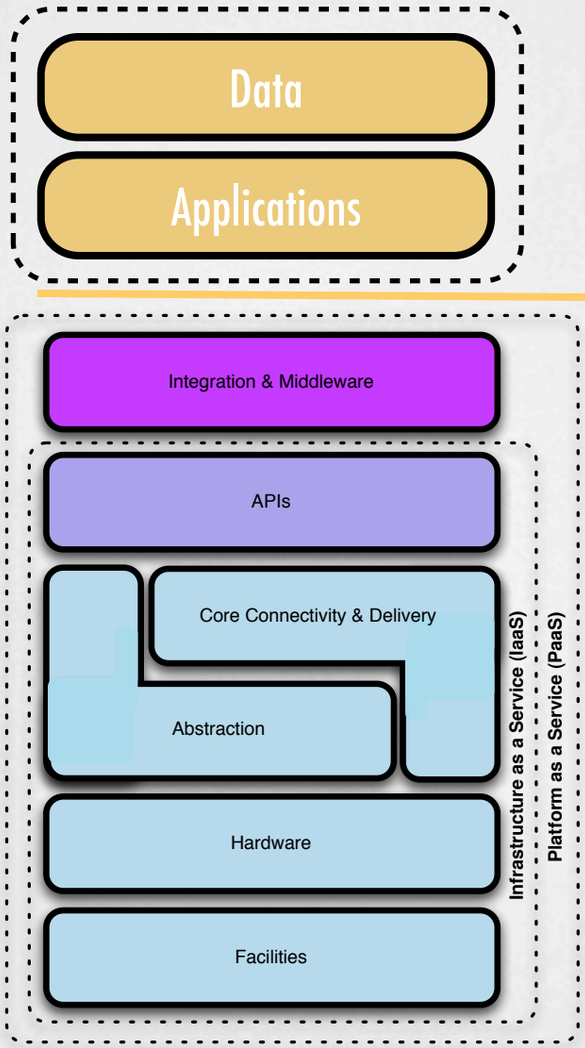
Network, Host & Storage Security



Consumer

Provider

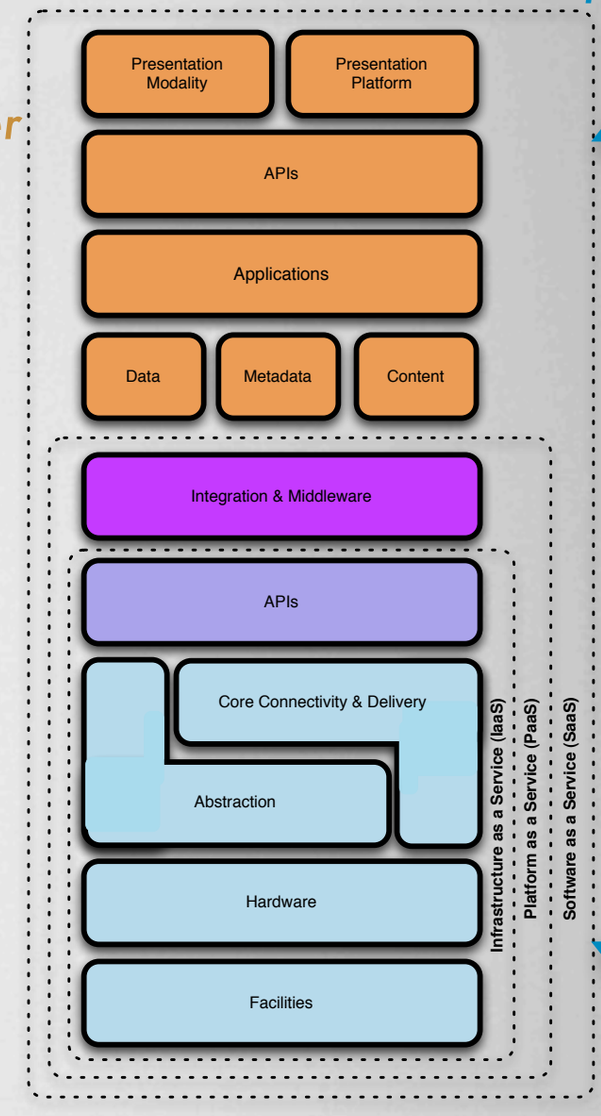
Application Security



Consumer

Provider

Information Security



Provider

IaaS

PaaS

SaaS

...Separately Based On Technology & Who Operates Them

The Stack

- **Infostructure**
  - Content & Context - Data & Information
- **Applistructure**
  - Apps & Widgets - Applications & Services
- **Metastructure**
  - Glue & Guts - IPAM, IAM, BGP, DNS, SSL, PKI
- **Infrastructure**
  - Sprockets & Moving Parts - Compute, Network, Storage

There's No Discipline...

Infostructure

Applistructure

Metastructure

Infrastructure

Information Security

Application Security

Network Security
Host-based Security
Storage Security

...In Our Discipline

How To Get Kick-*aaS Automated Security

1. Design for Scale & Re-define Deployment scenarios
2. Traffic steering/Service insertion/context - Physical and Virtual
3. Standardize On Common Telemetry & Consistent Policy Across Platforms
4. More intelligence shared between infra-/ Applistructure
5. Leverage guest-based footprint (IaaS)
6. Leverage Hypervisor, platform & software APIs
7. Leverage virtualized & Cloud delivery models for security

The Basics

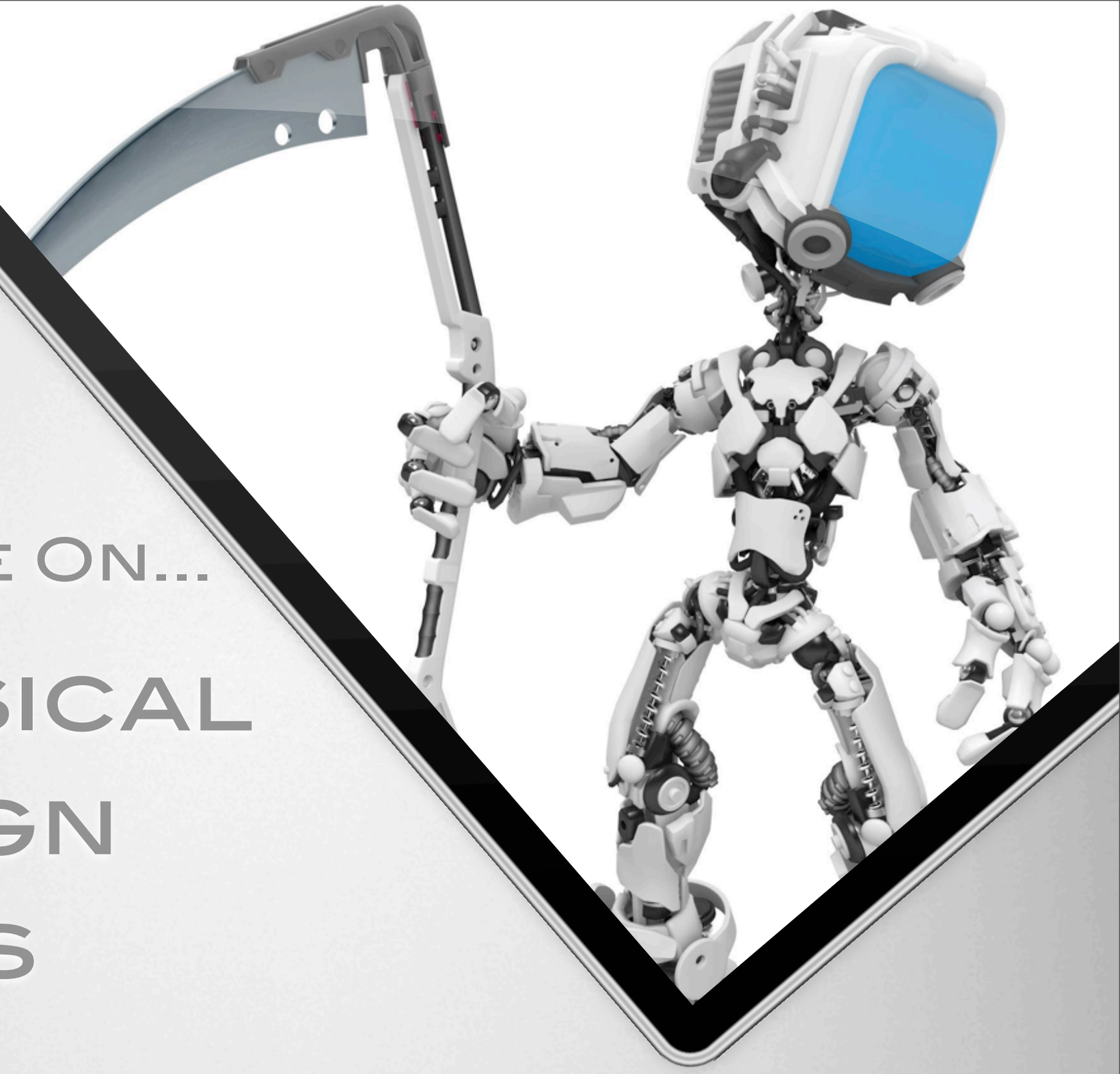
You <u>Still</u> Have To Manage The Basics:

- Building Survivable Systems
- Building Secure Apps
- Securing Data

You Also can't Expect the Cloud/ Virt Platform Providers to Give you All you need

Recognize, Accept & Move On...

The Classical DMZ Design Pattern Is Dead

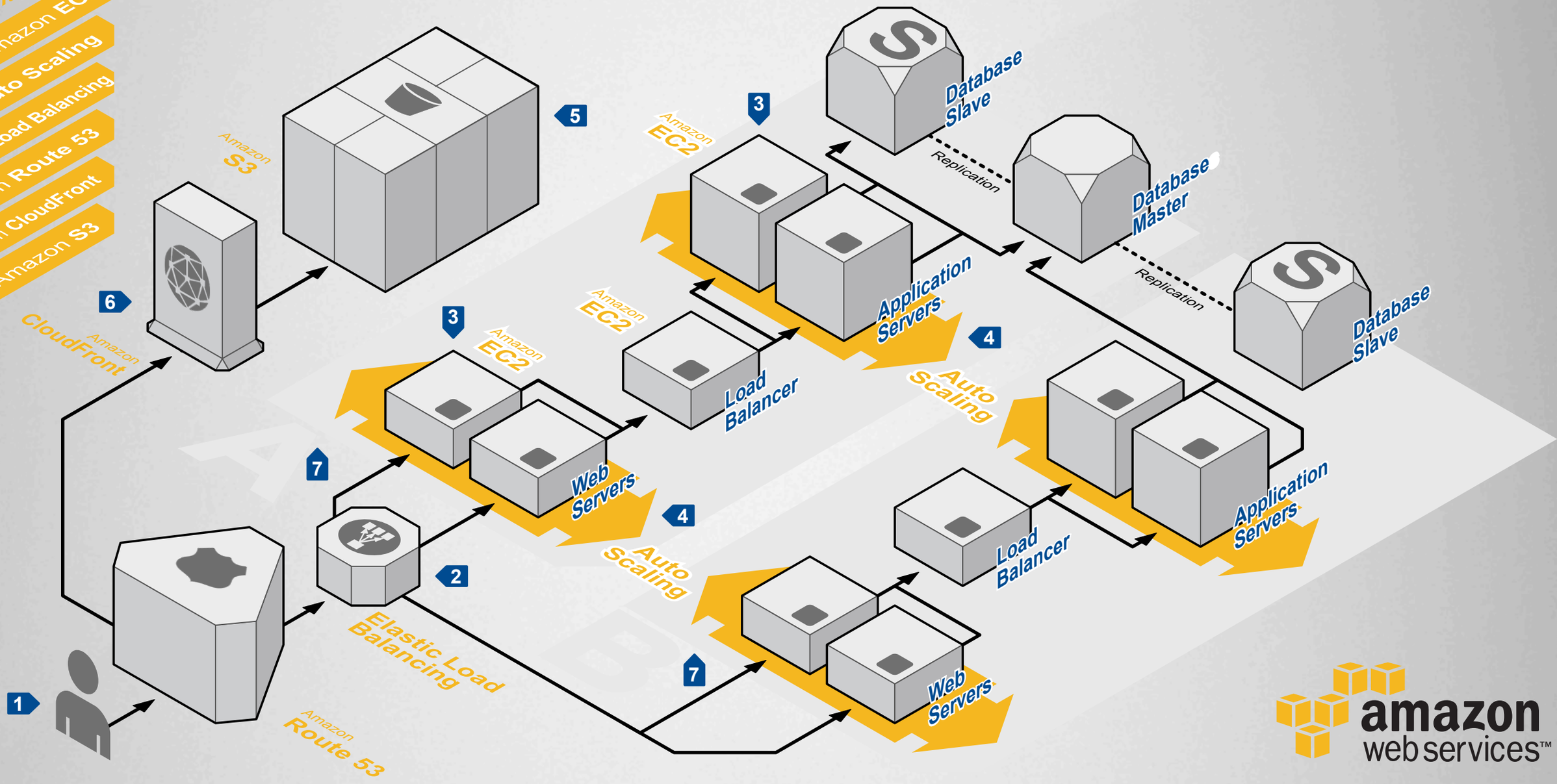


WEB APPLICATION HOSTING

Highly available and scalable web hosting can be complex and expensive. Dense peak periods and wild swings in traffic patterns result in low utilization rates of expensive hardware. Amazon Web Services provides the reliable, scalable, secure, and high-performance infrastructure required for web applications while enabling an elastic, scale out and scale down infrastructure to match IT costs in real time as customer traffic fluctuates.

AWS Reference Architectures

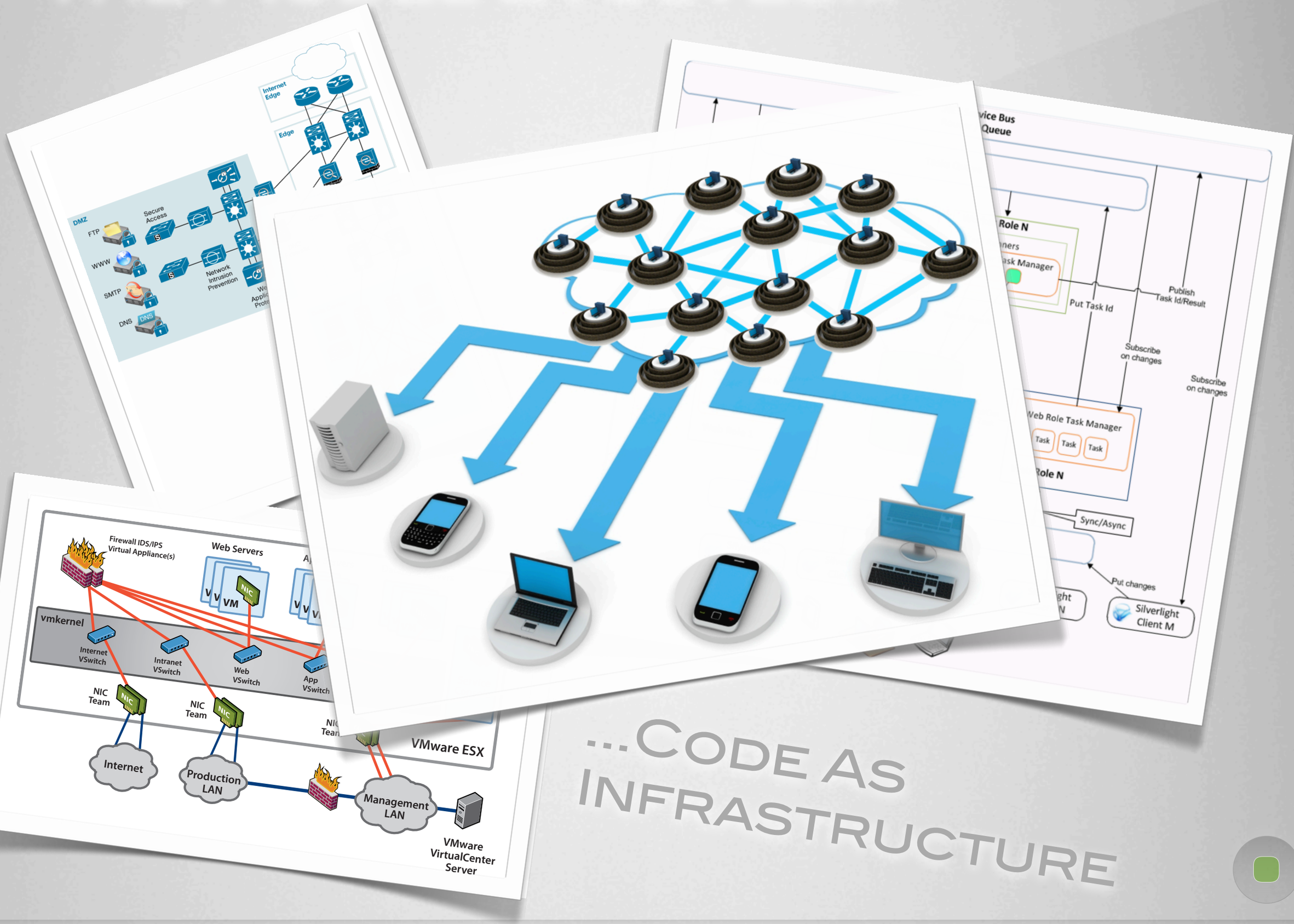
- Amazon EC2
- Auto Scaling
- Elastic Load Balancing
- Amazon Route 53
- Amazon CloudFront
- Amazon S3



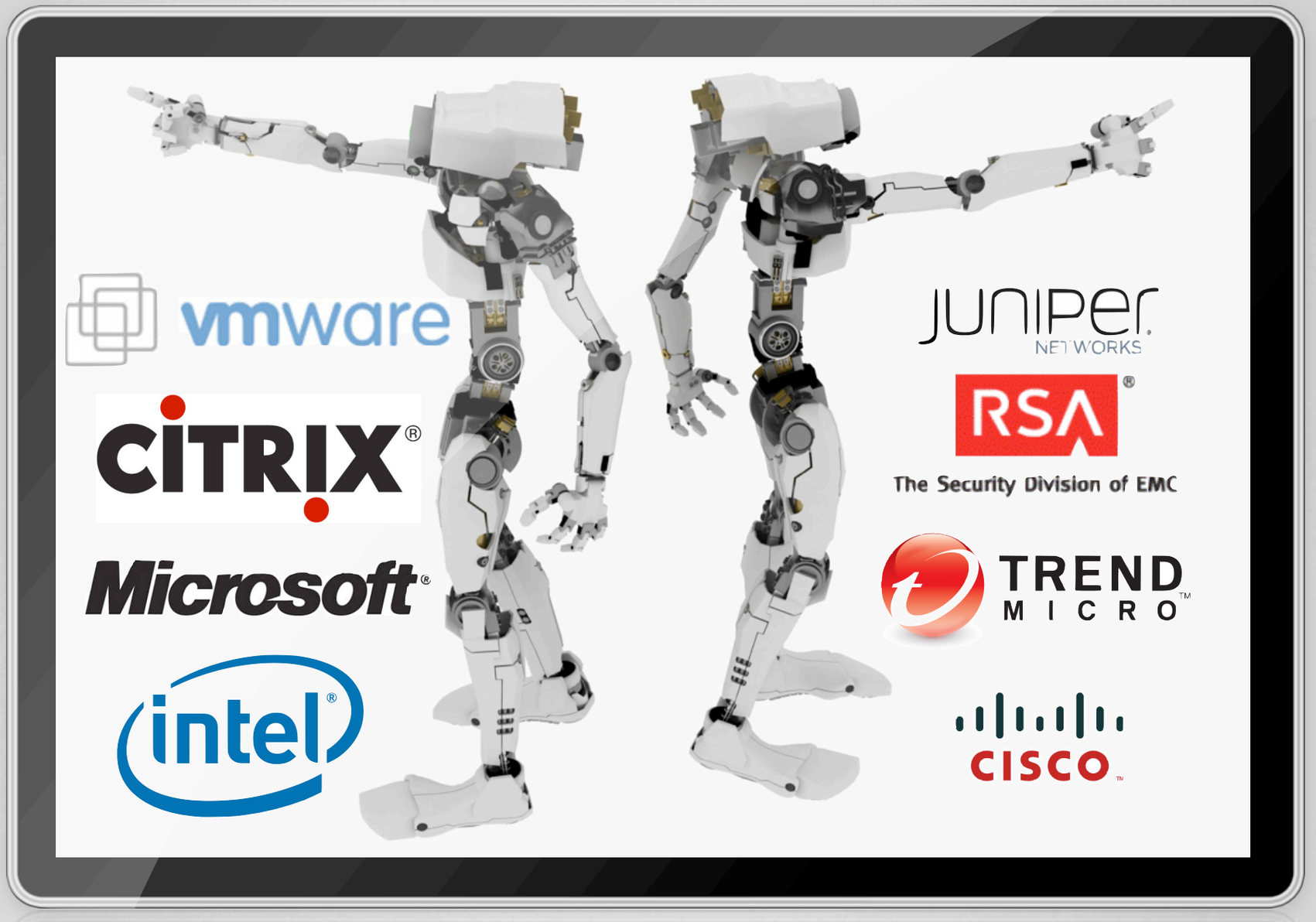
amazon web services™

LOOKS FAMILIAR, BUT...

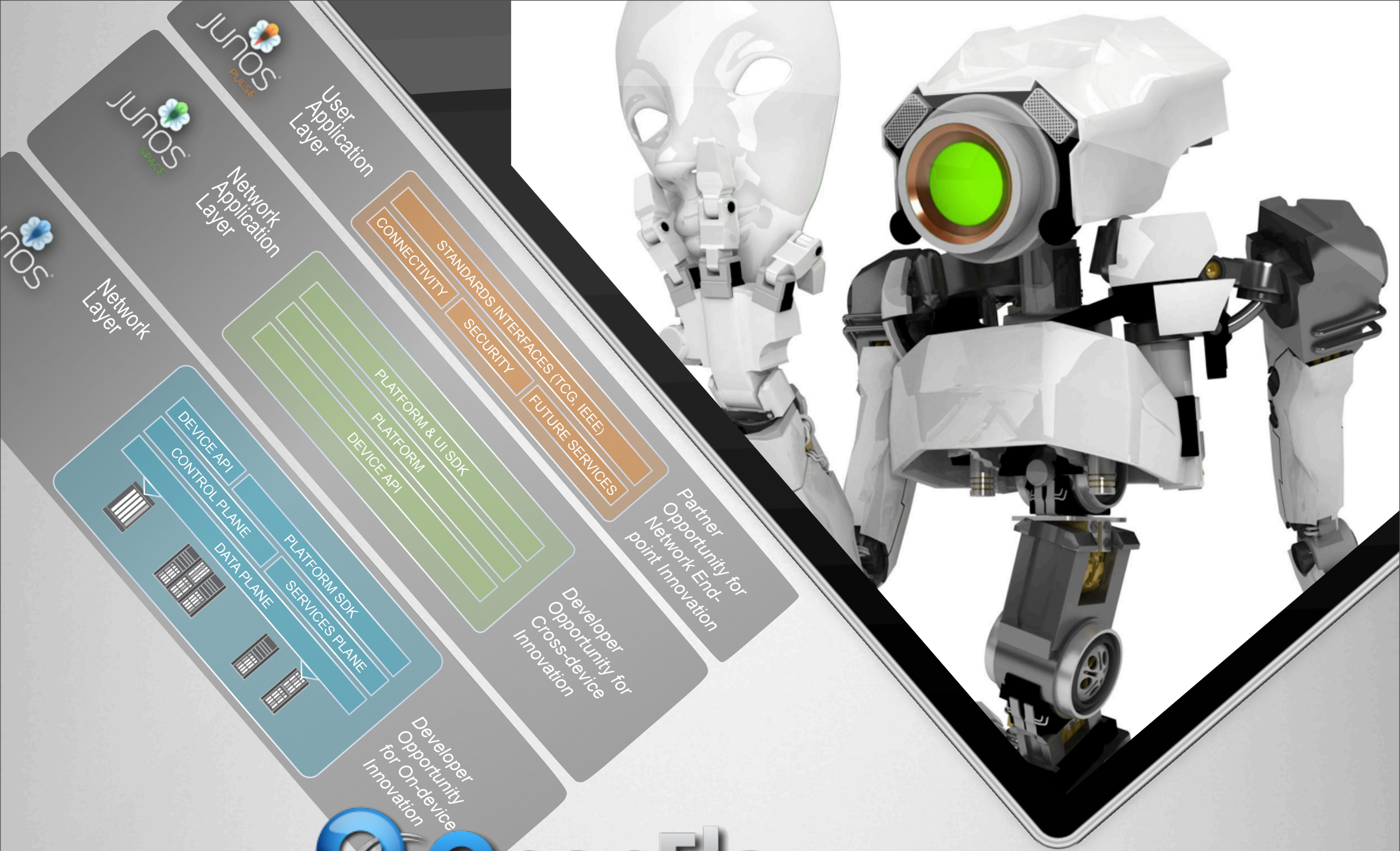
The Model Evolves...



...Code as Infrastructure



Where Should Security Be Delivered? Hardware, Virtualization/Cloud Platform Or Ecosystem?



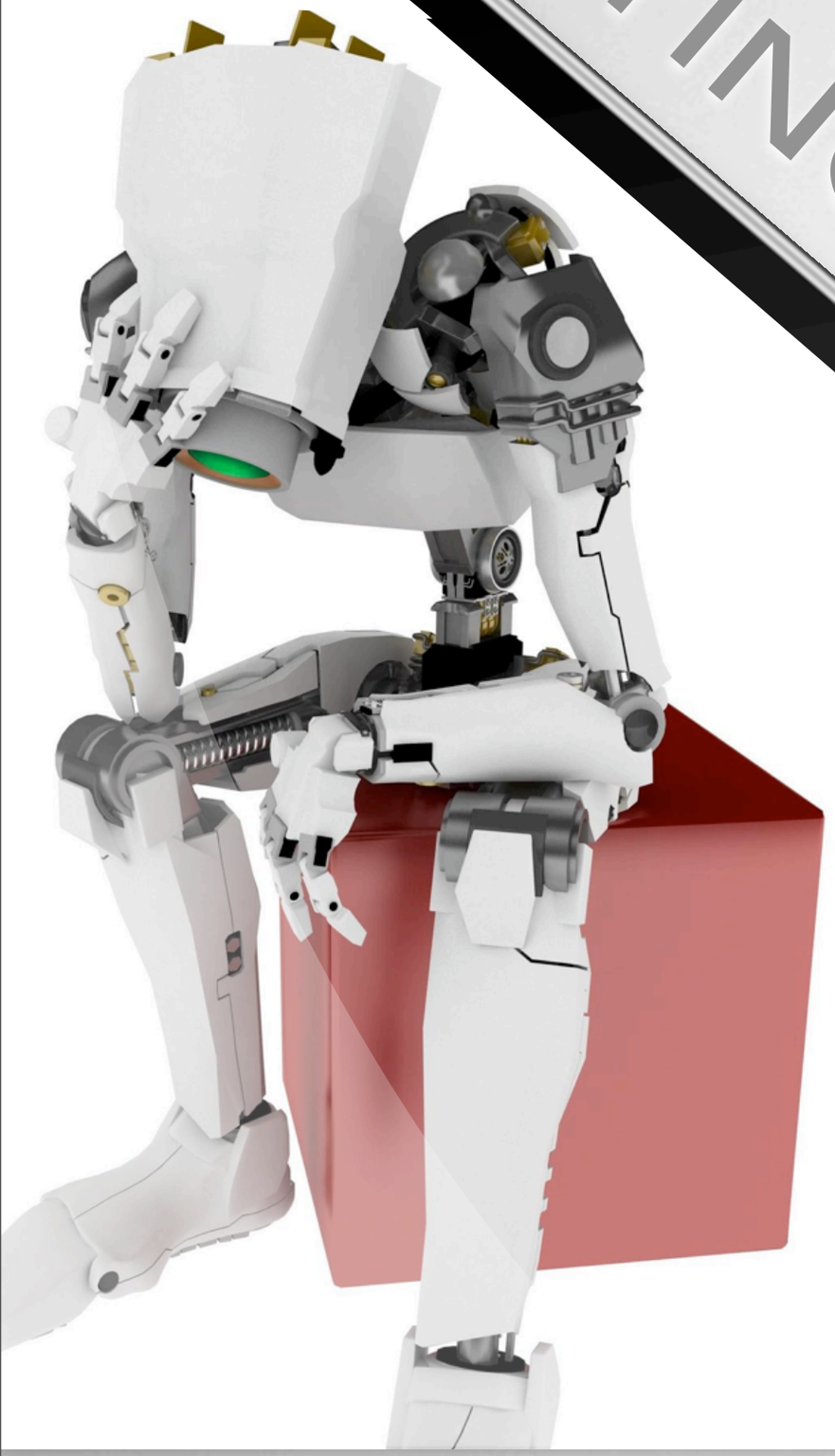
PROGRAMMABILITY...

Demand & Use Programmatic Interfaces (P.O.S.) From Security Solutions

AppSec/SDLC Is Huge

Devs Don't Necessarily make good security and vice versa

Getting There?



Automating Data Protection:

The Final Frontier...

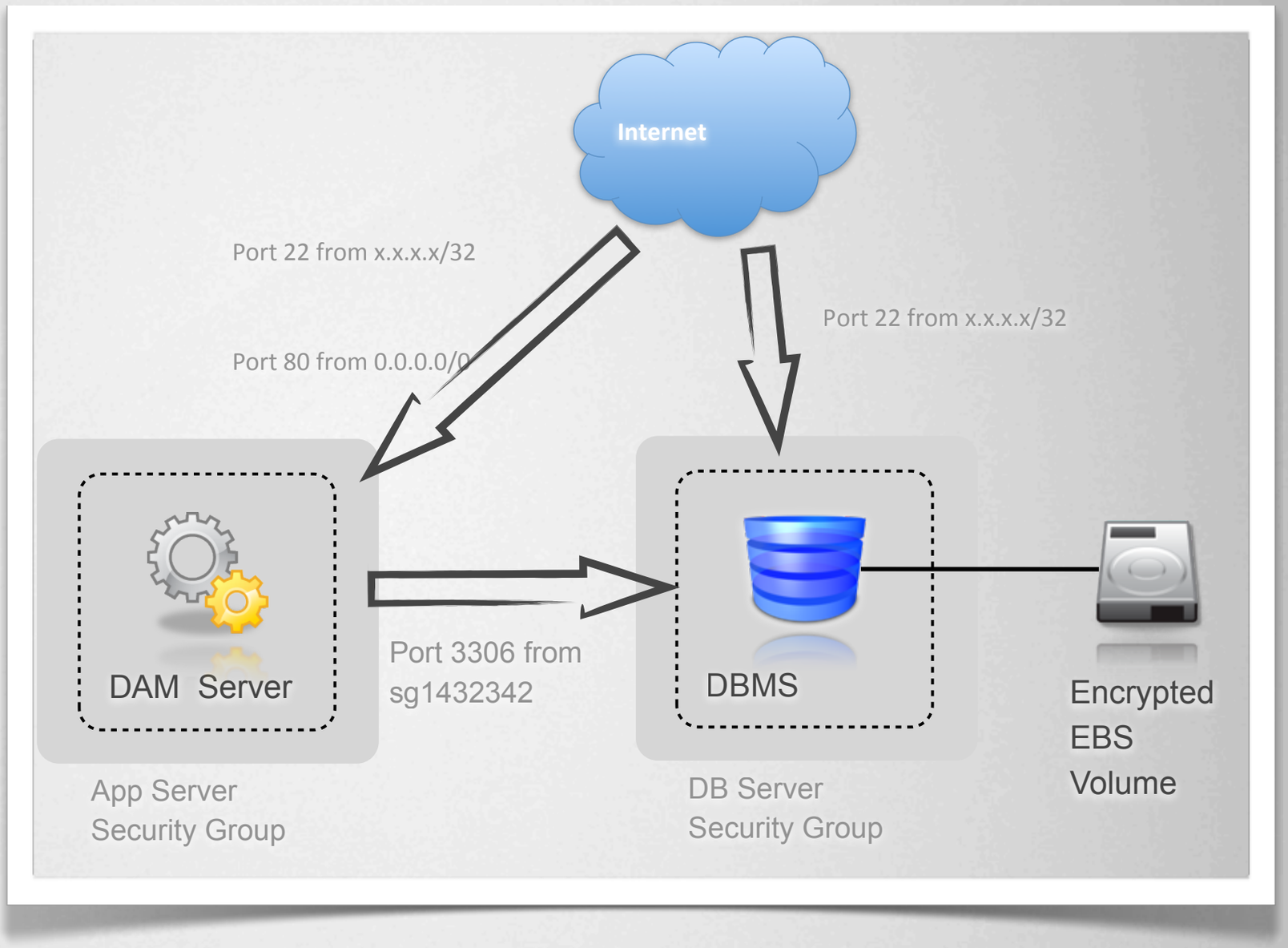
Solutions You Can Use Today

The Stack

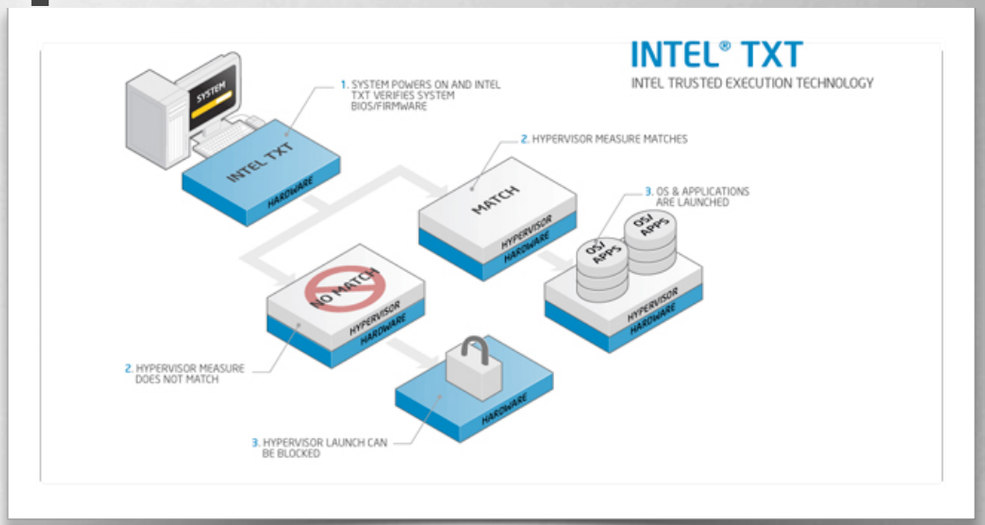
- **Infostructure**
  - Content & Context - Data & Information
- **Applistructure**
  - Apps & Widgets - Applications & Services
- **Metastructure**
  - Glue & Guts - IPAM, IAM, BGP, DNS, SSL, PKI
- **Infrastructure**
  - Sprockets & Moving Parts - Compute, Network, Storage

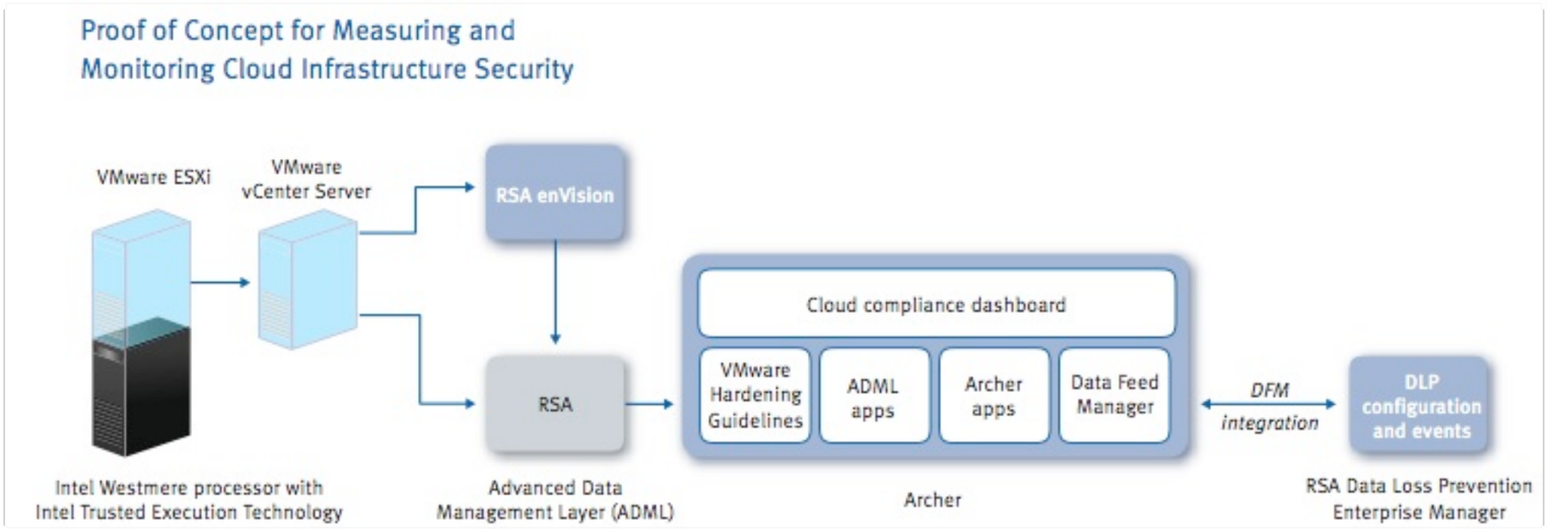
Cloudicornicopia

Segregation of service components is a natural artifact of cloud platforms

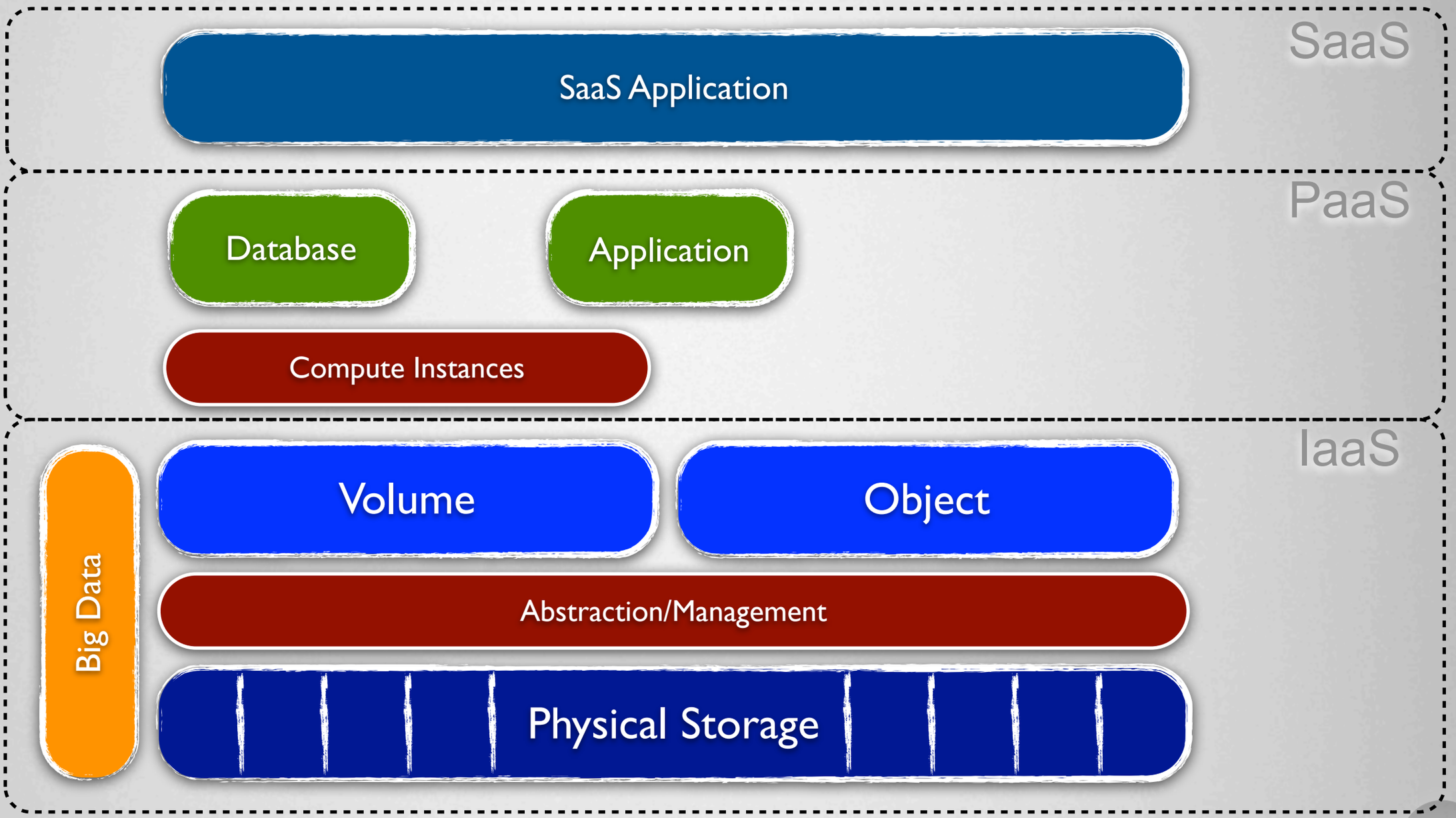


Foundational Level - CPU/Chipset

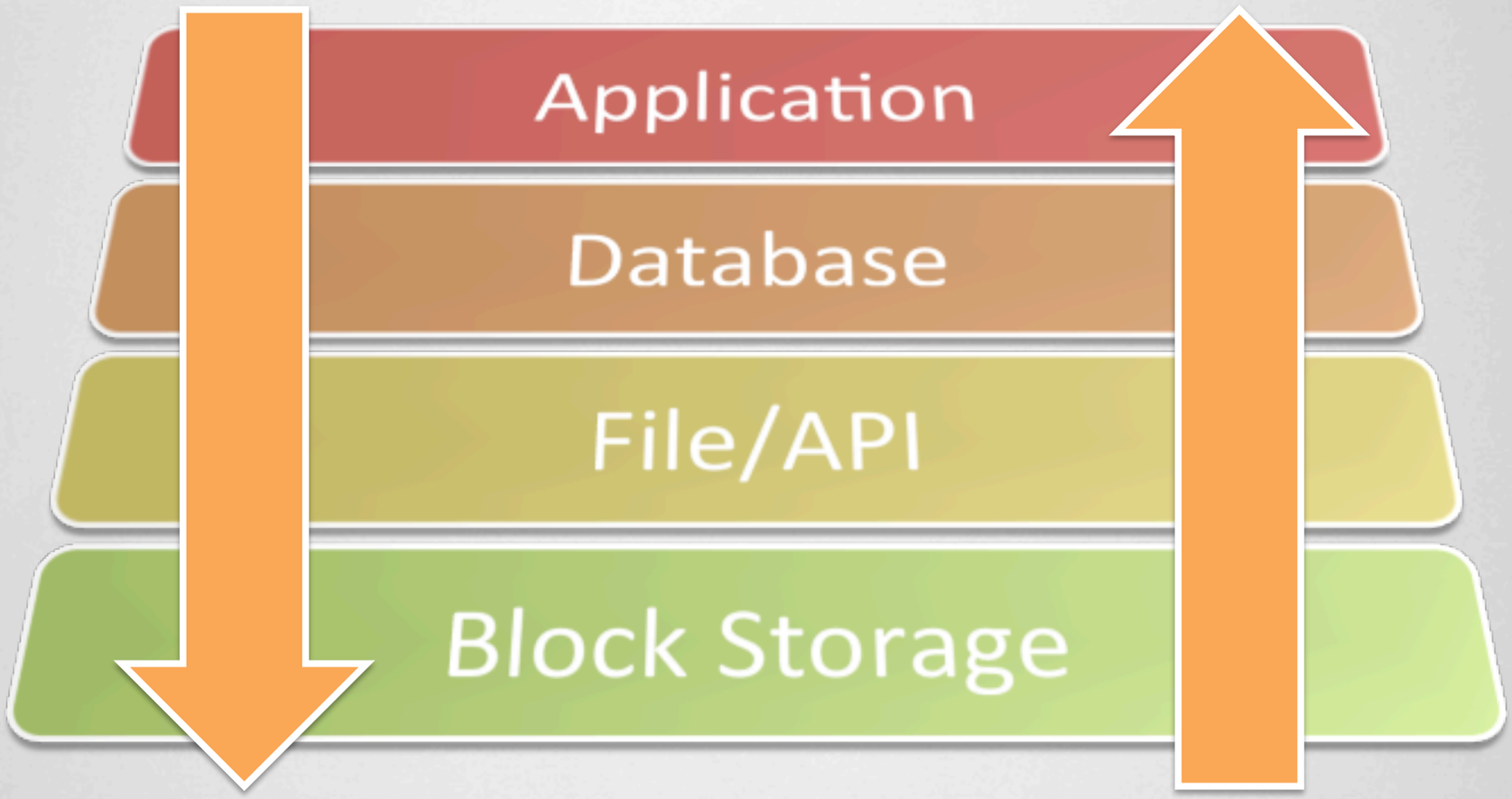




Cloud Data Architectures



Encryption Layers



IaaS Encryption Matrix

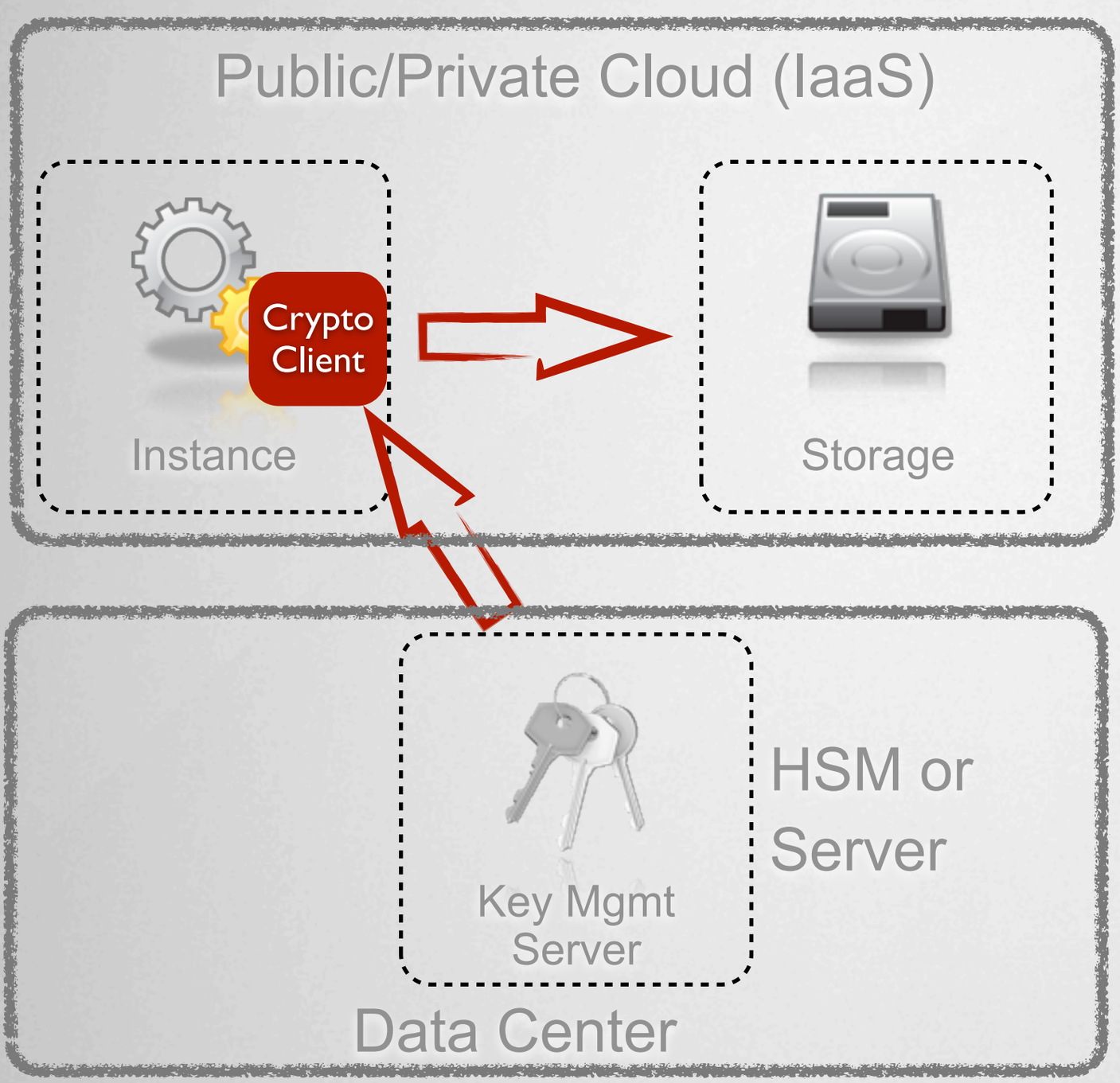
Components

- Encryption Engine
- Key Management
- Data Storage

Locations

- Instance
- Hardware
- Public
- Private
- Host
- Network

IaaS Distributed Encryption



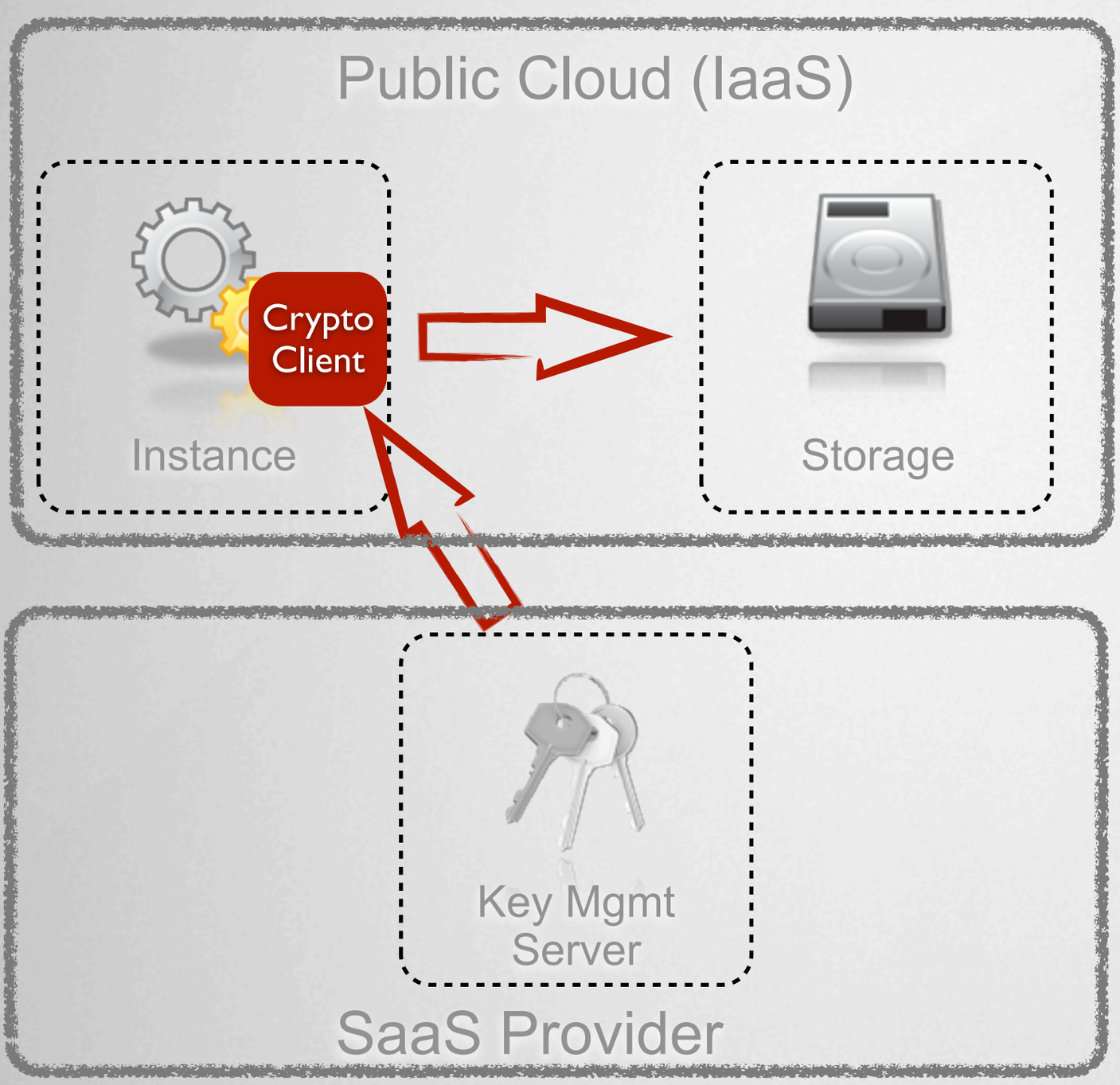
VORMETRIC

SafeNet

THALES

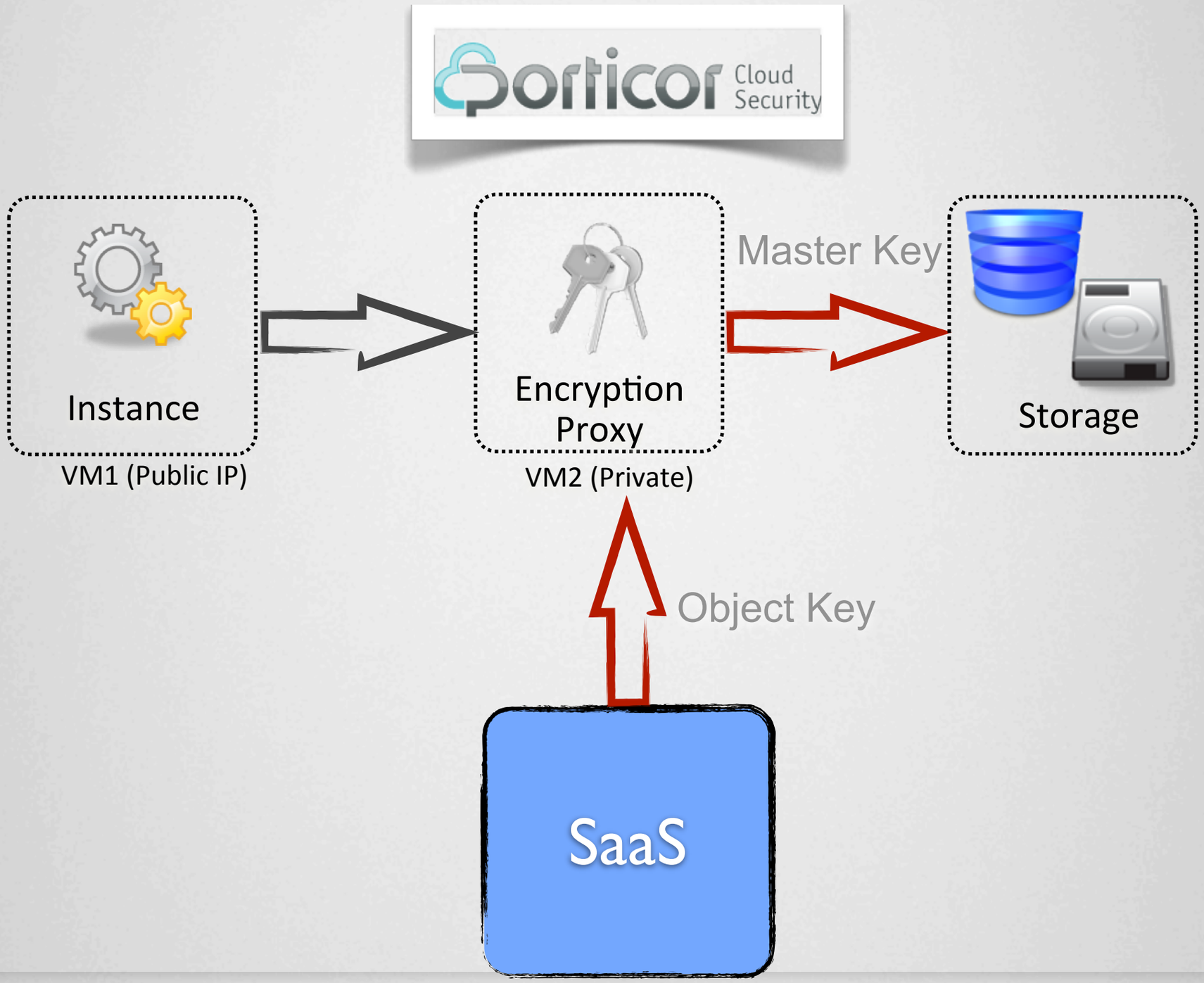
Voltage security

IaaS Distributed Encryption (SaaS)

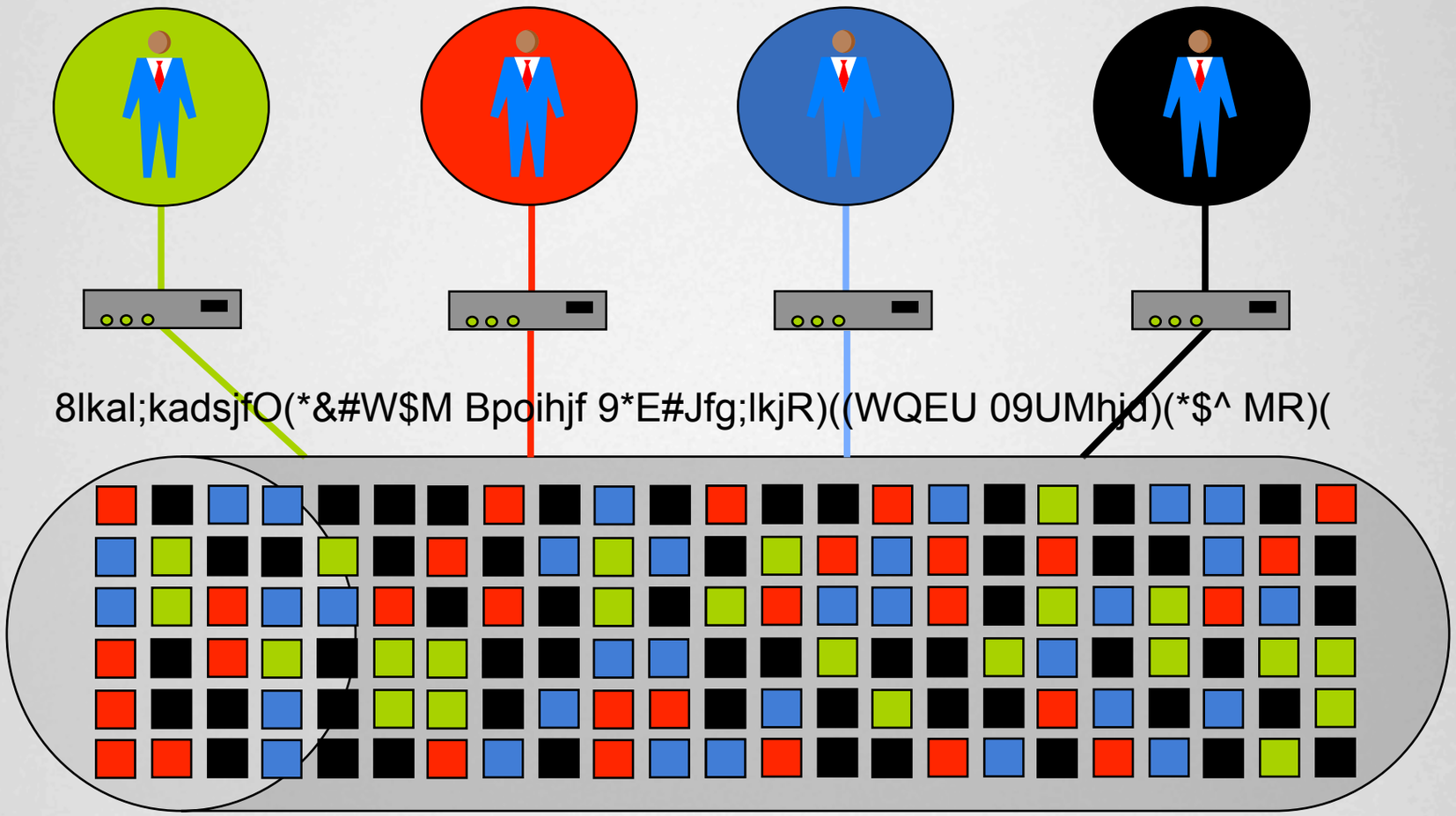


TREND MICRO

IaaS Proxy Encryption with Split Keys



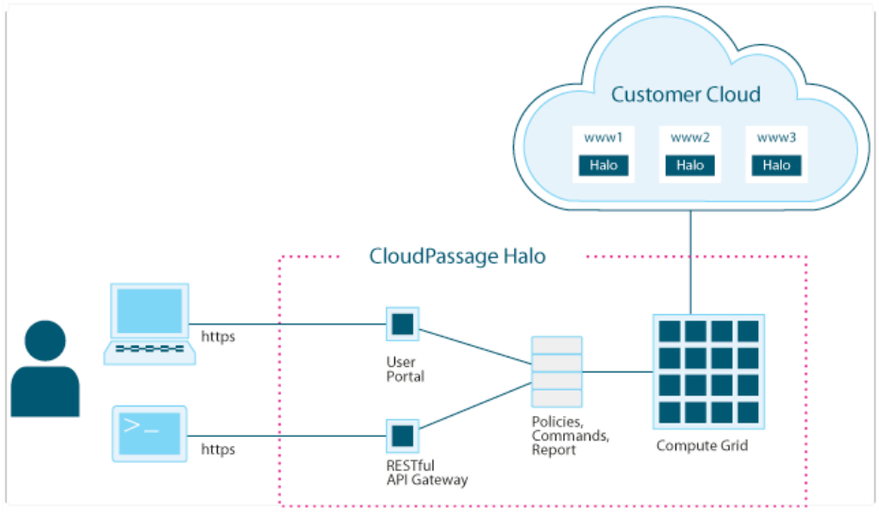
Virtual Private Storage

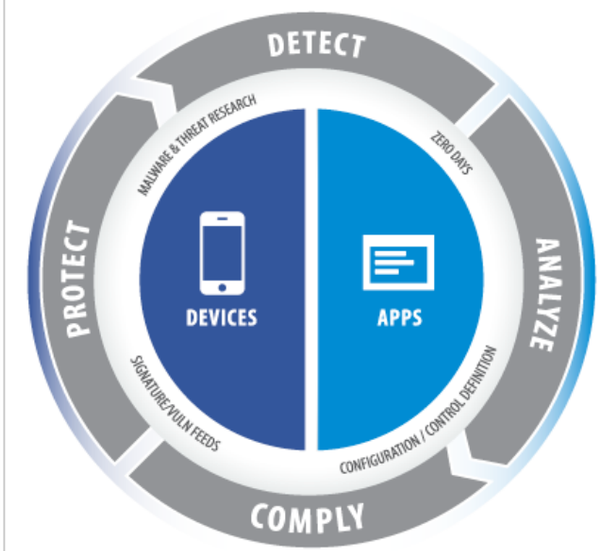


Shared Storage

AppSense Dropbox TRUECRYPT SOPHOS

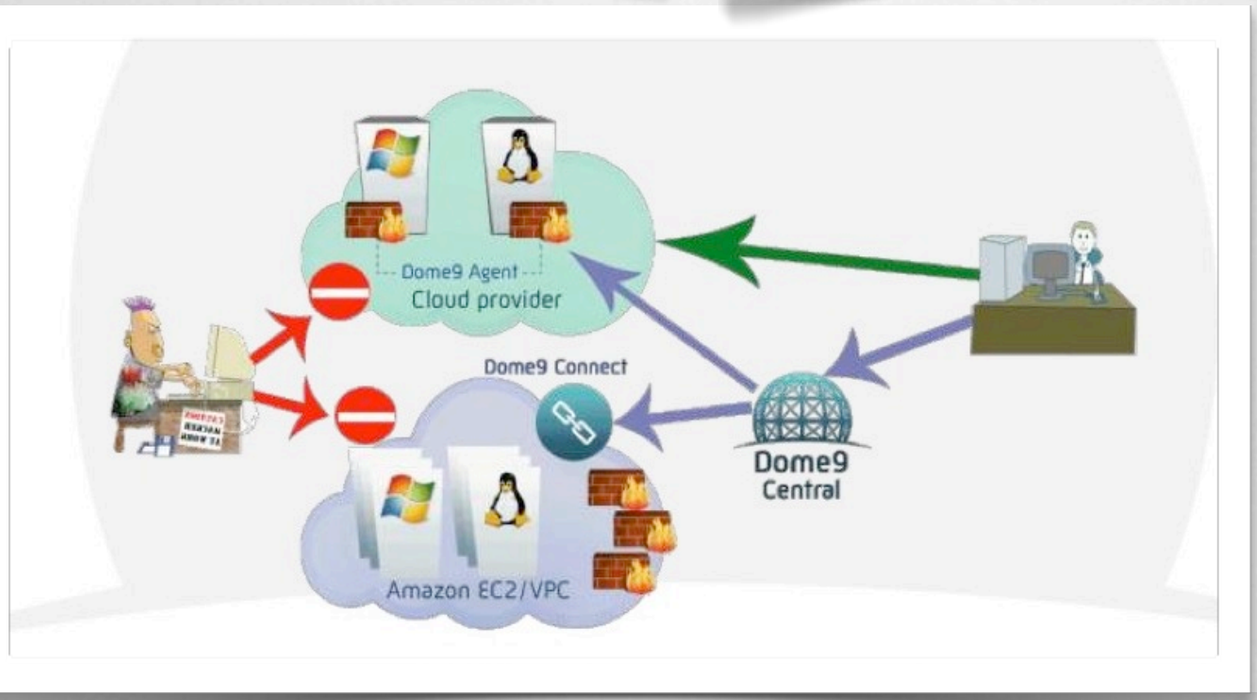
Security & Compliance Platforms





Dome9 SECURITY

CloudPassage

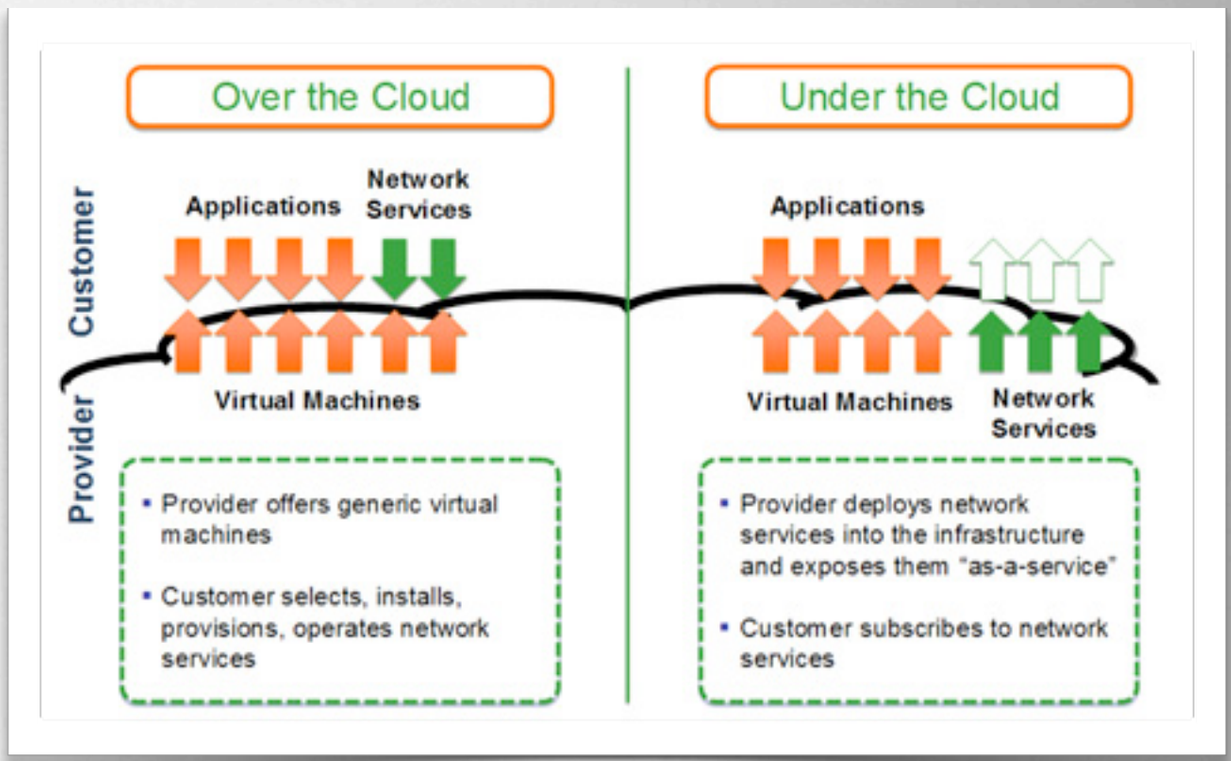


QUALYS

New Network Models & Security Solutions

- Network Virtualization & Software Defined Networking

- Networking Overlays



embrane
Powering the Agile Network

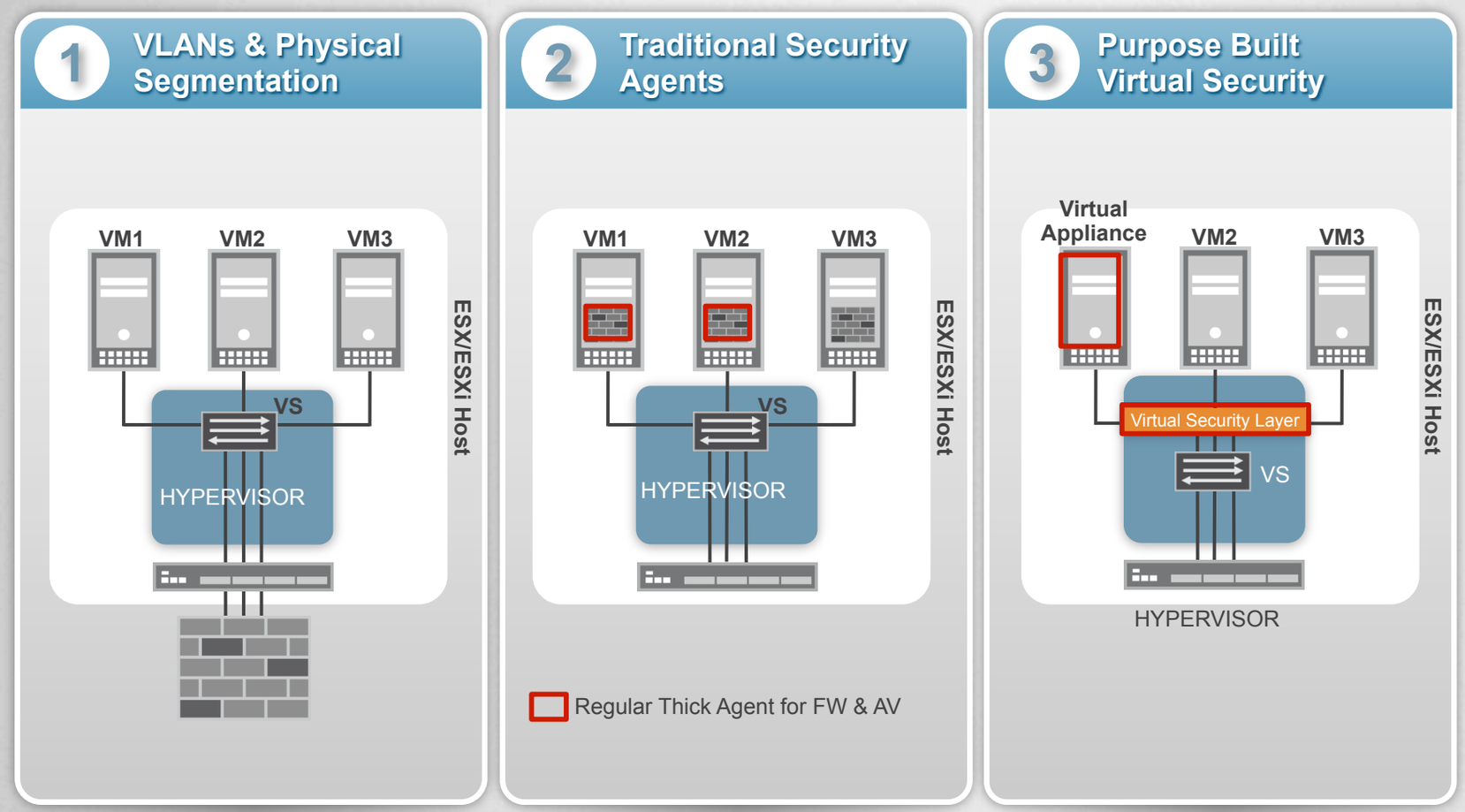
VCIDER

nicira

big switch networks

CLOUDSWITCH™

...Virtual Security Appliances & Introspection solutions



vmware

HyTrust
Virtualization Under Control

RSA
The Security Division of EMC

JUNIPER NETWORKS

TREND MICRO

CISCO

reflex

catbird

The Stack

- **Infostructure**
  - Content & Context - Data & Information
- **Applistructure**
  - Apps & Widgets - Applications & Services
- **Metastructure**
  - Glue & Guts - IPAM, IAM, BGP, DNS, SSL, PKI
- **Infrastructure**
  - Sprockets & Moving Parts - Compute, Network, Storage

Management, provisioning, orchestration, Governance

The Enterprise Cloud Management Solution

bluelock. EMC² GOGRID
amazon web services terremark CloudSigma vmware openstack
Windows Azure nimbula EUCALYPTUS cloudcentral SERVER EXPRESS
cloudstack JoyentCloud rackspace HOSTING Google at&t

Console

API

enSTRATUS
SaaS or On-premise

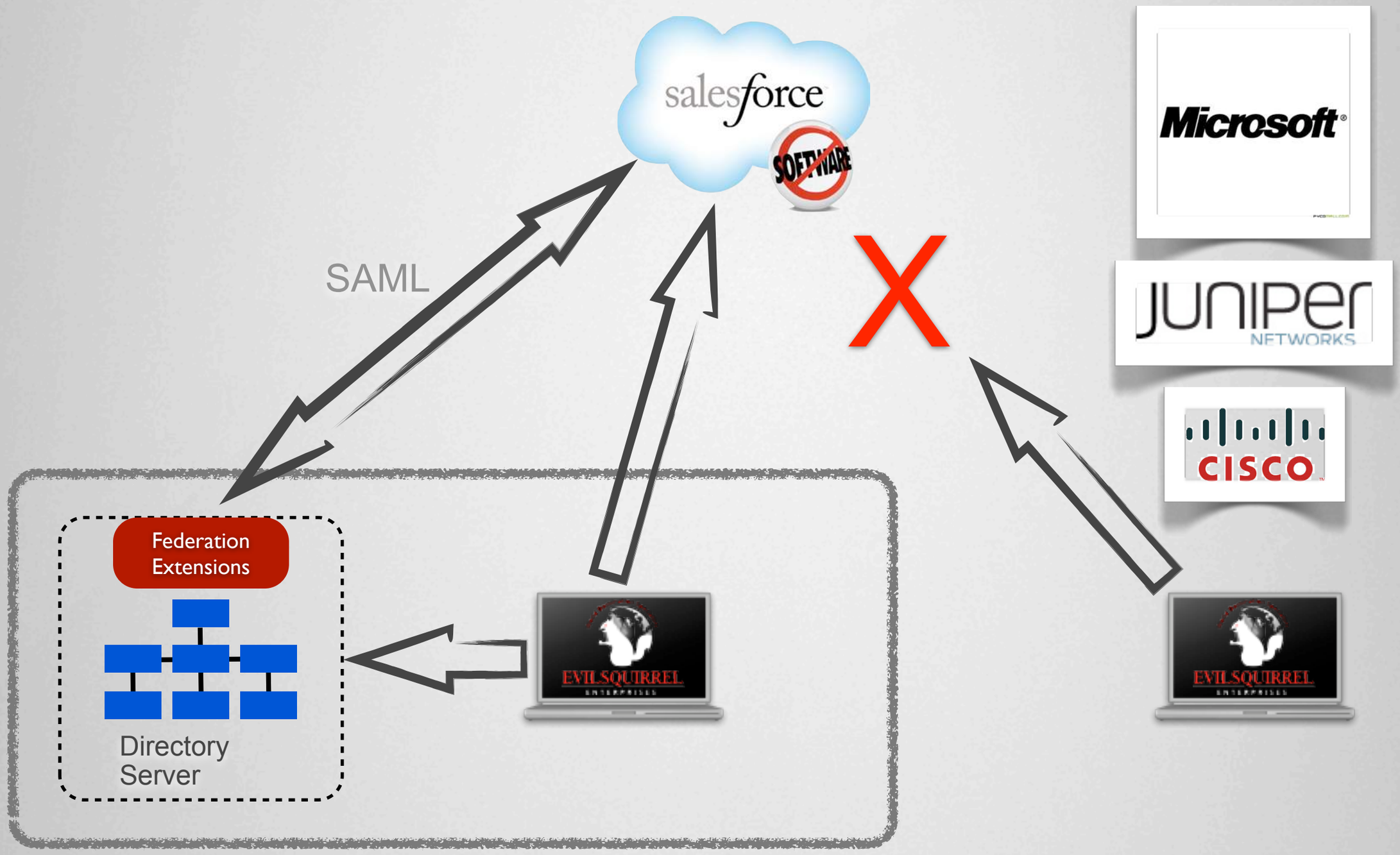
API

- Unified management
- Granular access controls
- Financial controls and chargeback
- Security & encryption
- Automation: in & cross cloud

Access directory service	Identity authentication	Project budgeting	Pricing & metering	Billing	…
Service delivery catalog	Change & config. mgmt.	Incident & problem mgmt	Security policy mgmt.	…	…

enSTRATUS

Restricting Device/ Location with Federation



Federation Gateways

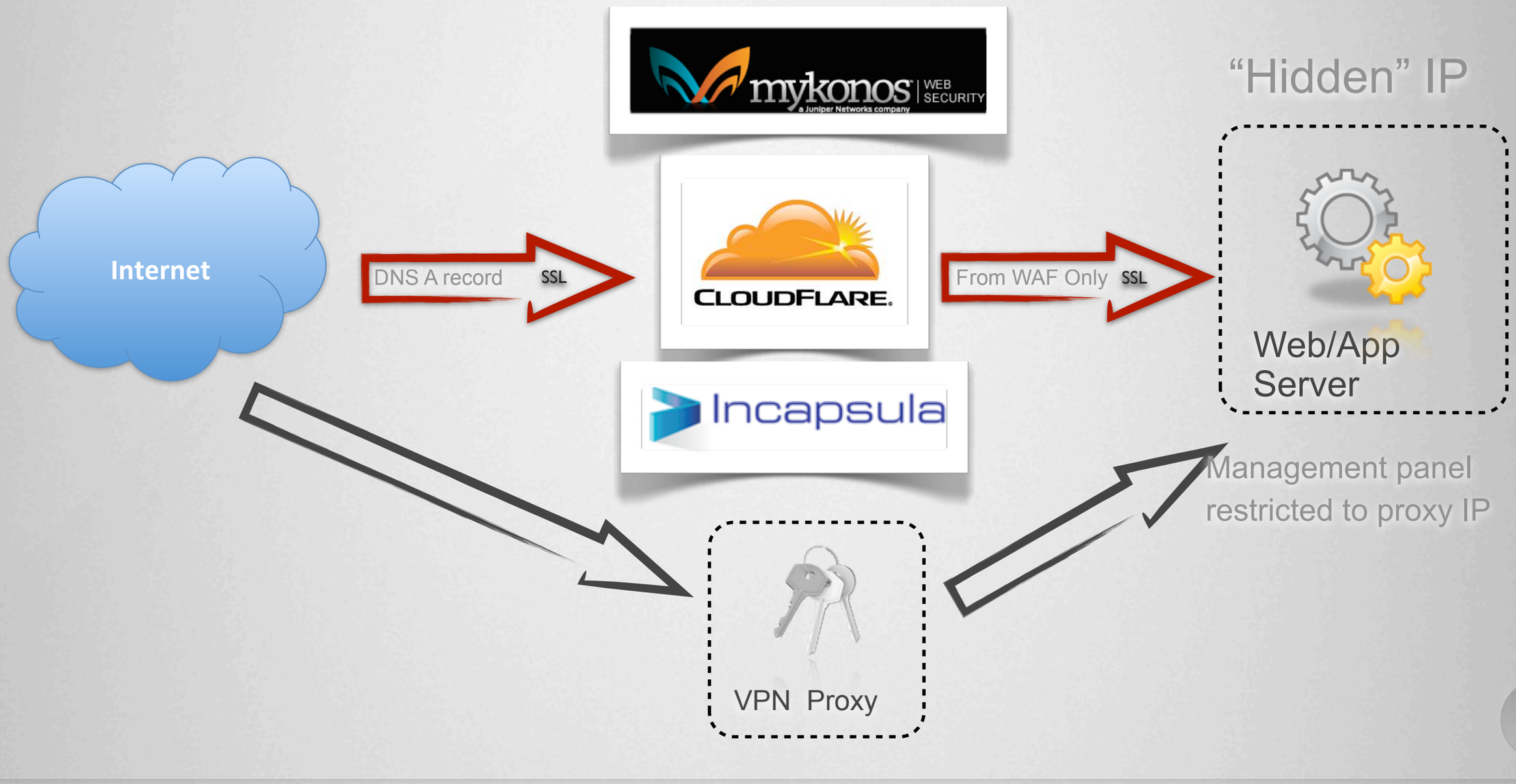
The Stack

- **Infostructure**
  - Content & Context - Data & Information
- **Applistructure**
  - Apps & Widgets - Applications & Services
- **Metastructure**
  - Glue & Guts - IPAM, IAM, BGP, DNS, SSL, PKI
- **Infrastructure**
  - Sprockets & Moving Parts - Compute, Network, Storage

New Models

- Intrusion Deception
- Scaleable Cloud AppSec
- Anti-malware Threat intelligence
- Security-as-a-Service

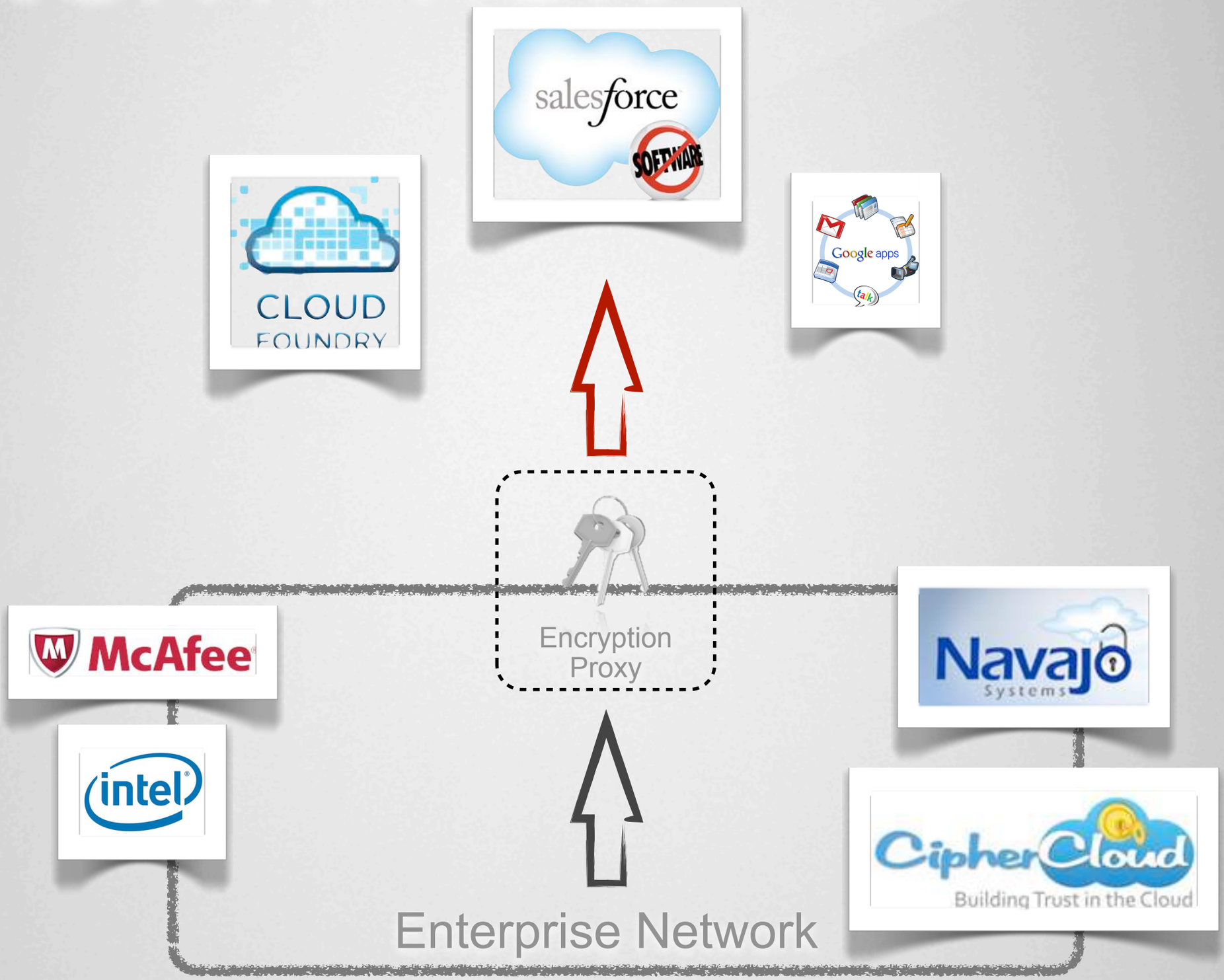
Cloud WAF = WAF + DDoS + Stats + Bandwidth Optimization + IPS



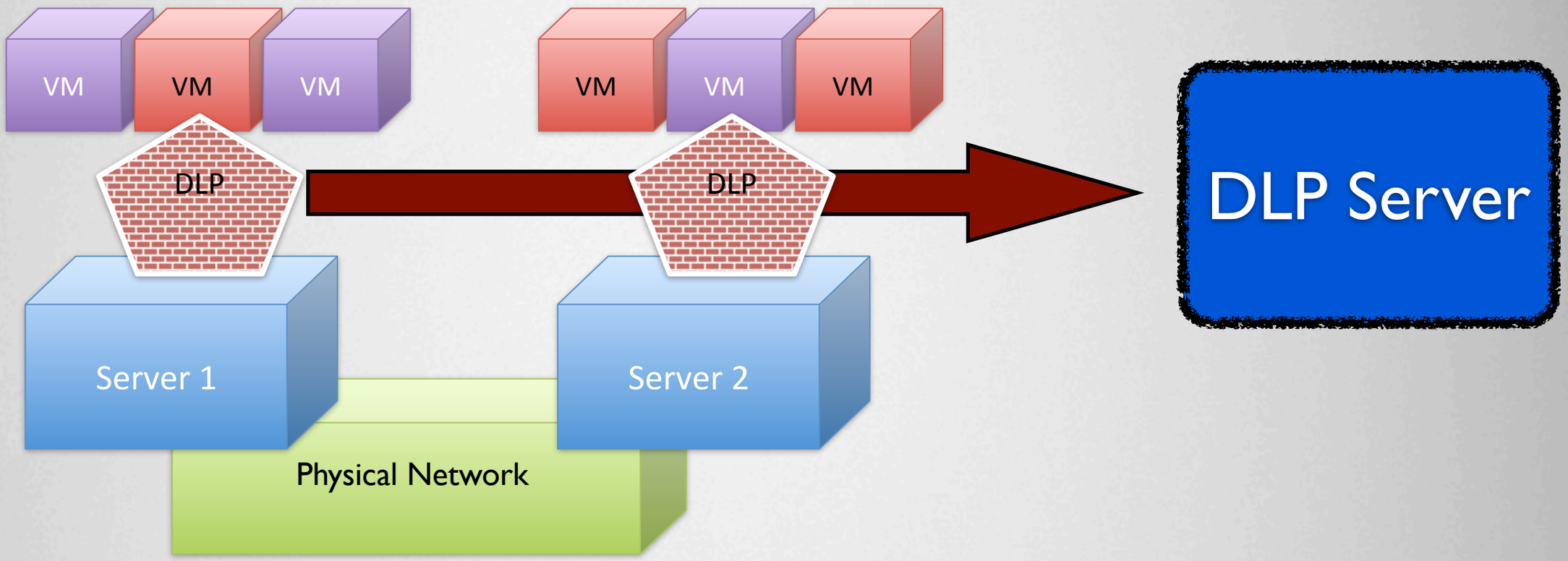
The Stack

- **Infostructure**
  - Content & Context - Data & Information
- **Applistructure**
  - Apps & Widgets - Applications & Services
- **Metastructure**
  - Glue & Guts - IPAM, IAM, BGP, DNS, SSL, PKI
- **Infrastructure**
  - Sprockets & Moving Parts - Compute, Network, Storage

SaaS/PaaS Proxy Encryption



Hypervisor DLP

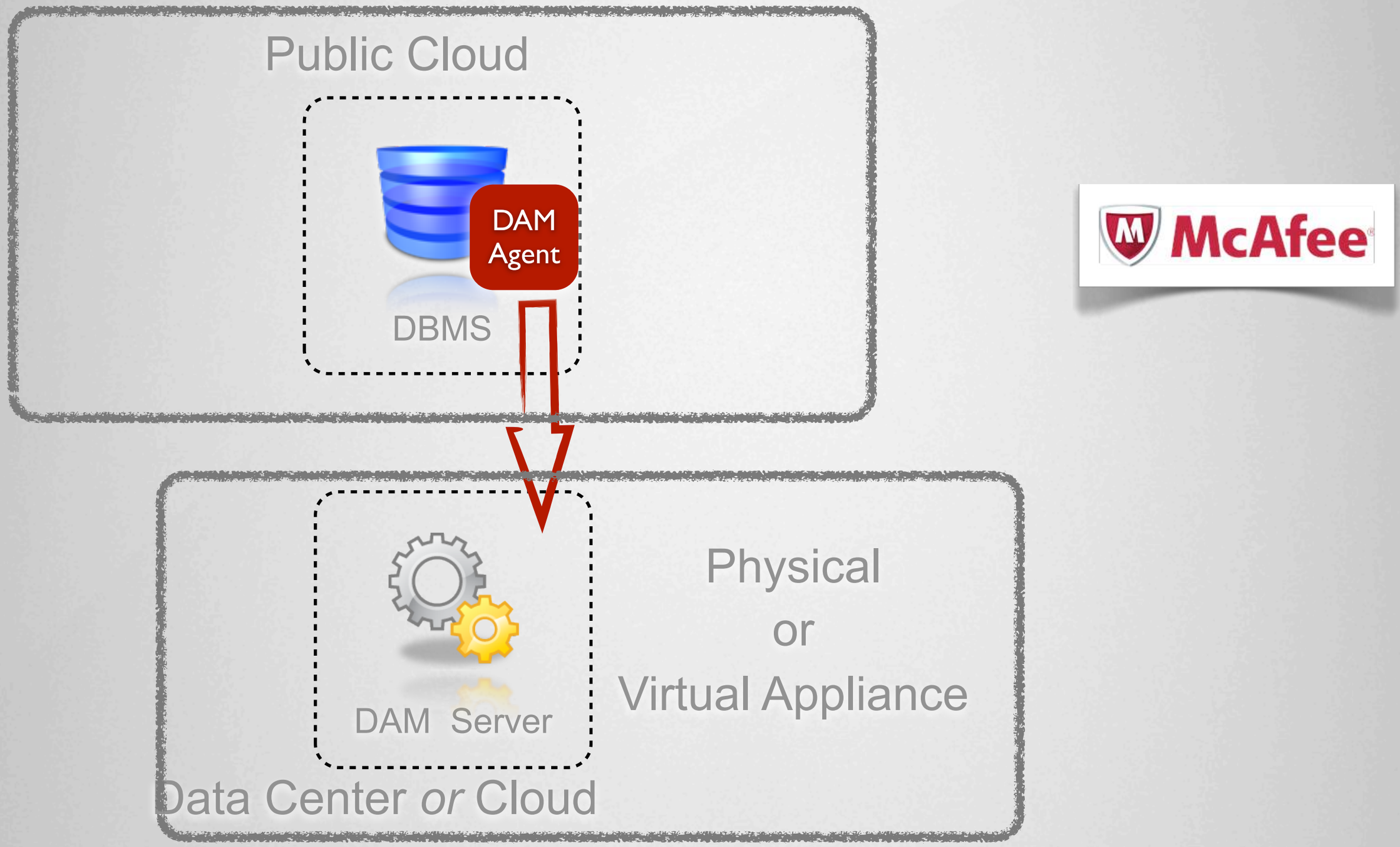


Discovery only (today)

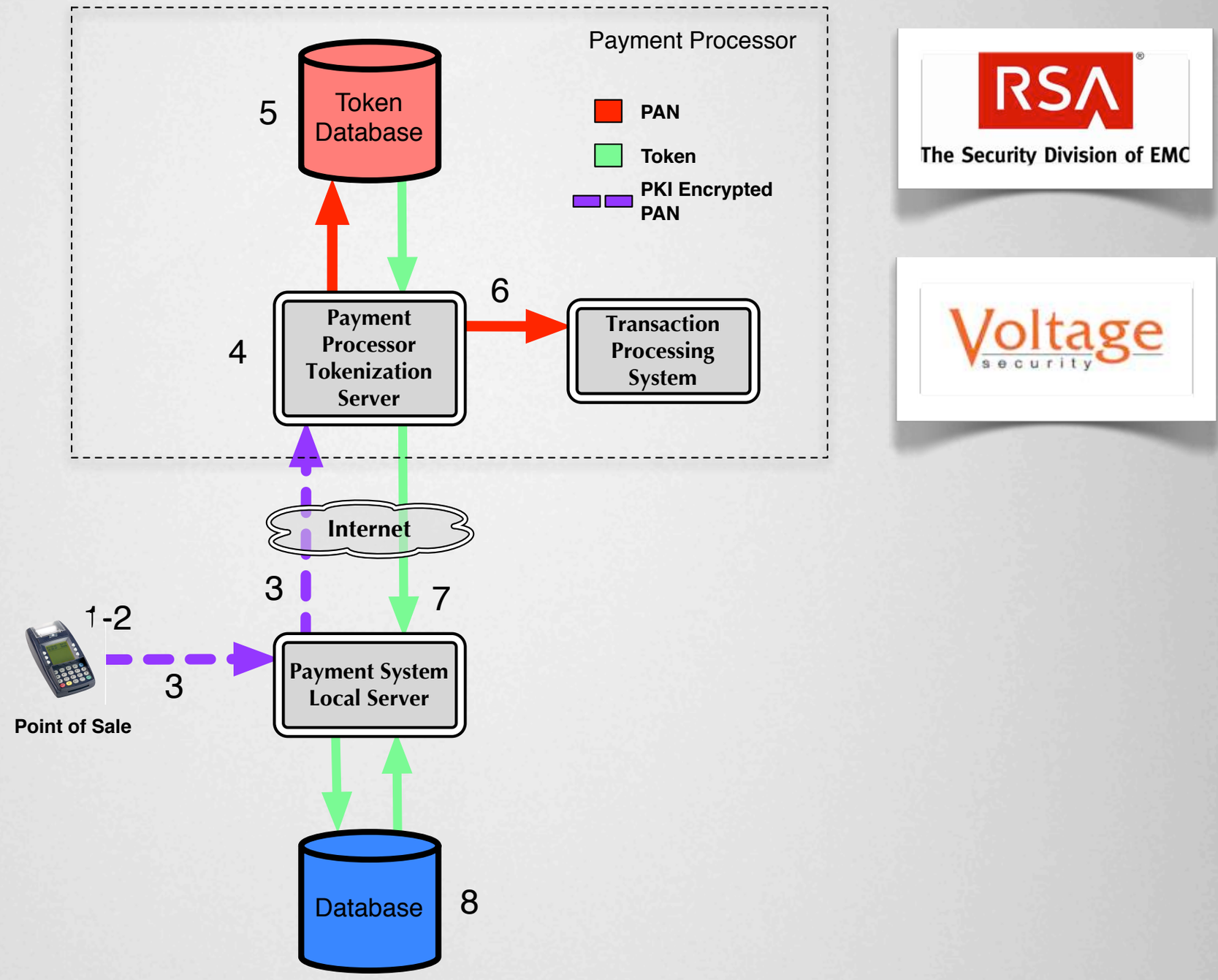
RSA
The Security Division of EMC

vmware

Database Activity Monitoring



SaaS Tokenization



RSA
The Security Division of EMC

Voltage security

Wrap-Up

The Punchline

- In The Simplest Of Terms, Using Cloud May Means Imagining Applications & Information Acro[illegible] Al[illegible] Ti[illegible] av[illegible] Potential To Be C[illegible]e[illegible] ct[illegible] The Internet...
- We Often Ca[illegible]t Trust The Provider, So We Must Engin[illegible]r S[illegible]urit[illegible]n[illegible] De[illegible]gn Patterns Acros[illegible] The[illegible]ntir[illegible] St[illegible]k
- Any “Dumb” Component In The Stack Compromises The Integrity Of the Entire Stack...
- APIs, Intelligence and Automation EVERYWHERE

HERE TODAY

The Future Of Security

- Content analysis fully integrated into both productivity and transaction applications.
- Ri[illegible] (and thus encryption) ap[illegible]ed at the point of creation, at the data element level.
- [illegible]ok[illegible]oint[illegible]etween on-p[illegible]mise[illegible]remise, and between [illegible]d ser[illegible]es enforce policies at the [illegible]ta [illegible]el, enforced by encryption/DRM.
- Policies and rights transfer and are maintained between state, phase and platform changes.

HERE TODAY

Photo by Caneles - http://flic.kr/p/4SGcdj

Securosis

DevOps Chops

- Still An Integrator's Dilemma, but getting better every day

- You're going to have to change what you do and what you do it with

- Embrace Automation, APIs and Agile

- Solutions are deployable <u>today</u>

Mogull

Securosis, L.L.C.

rmogull@securosis.com

http://securosis.com

AIM: securosis

Skype: rmogull

@rmogull

Hoff

Juniper

choff@packetfilter.com

choff@juniper.net

http://www.rationalsurvivability.com/blog

AIM: {How 1980's!}

Skype: infosecenigma

@Beaker