Innovation in the Cloud and the Importance of Security

Steve Chappell COO & EVP Sales and Marketing

THE Meeting Place for Technology Leaders

wedge networks
securing the cloud connected world

Agenda

- For security…there's opportunity in the Cloud
- The New Connectivity Paradigm
- Implications for Security
- The Road Ahead: Security via SDN and NFV
- Requirements for Success
- What's in it for the Service Provider?

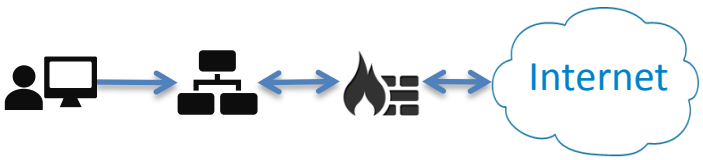
A Do-Over for Security?

- Despite concerns….the disruption of the Cloud actually presents a fresh opportunity to rethink security

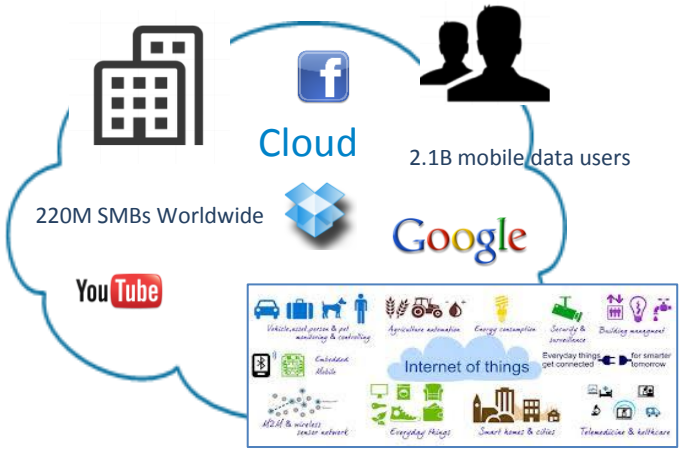
- As NFV and SDN look to enable the Cloud new possibilities for designing security into the network exist

Cloud Implications for Networking & Security

Old Connectivity Paradigm



New Connectivity Paradigm



All of today's mainstream security products are designed to function within the old network connectivity paradigm

Result: Existing Solutions Can't Protect Today's Cloud-Connected World Against Evolving Threats

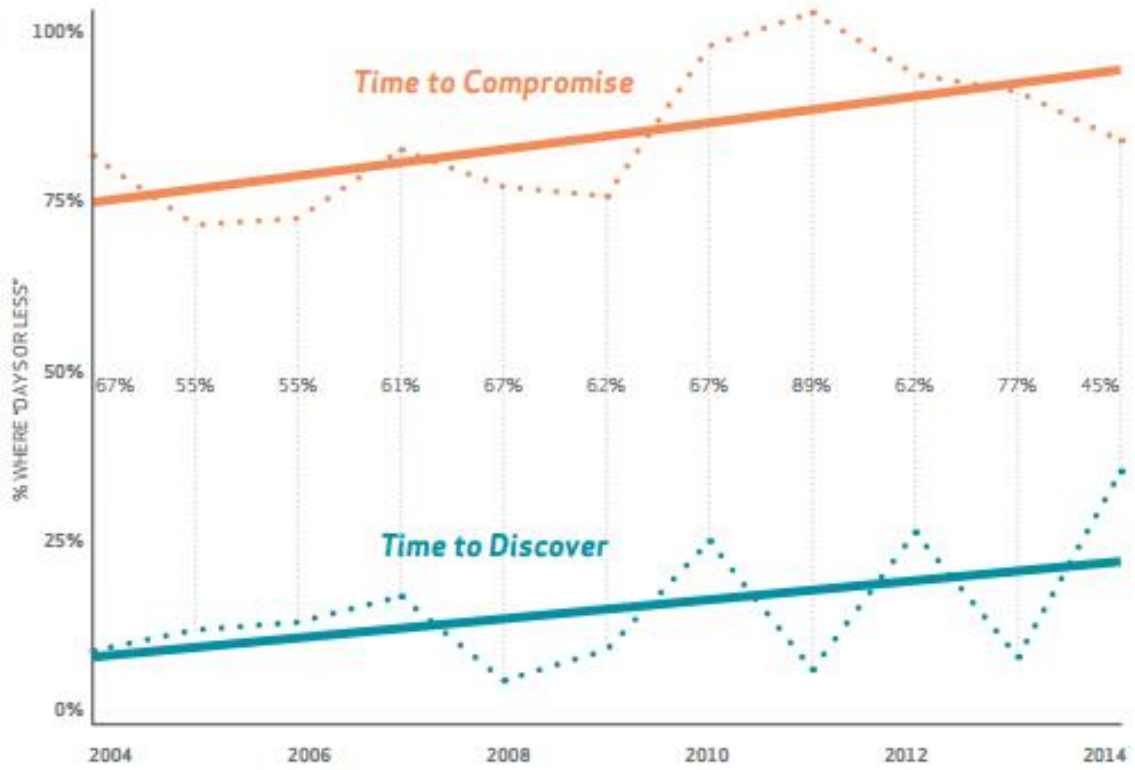
wedge networks
securing the cloud connected world

Shortcomings of Existing Security Alternatives

First Generation Products (Premise or Cloud Assisted), Dedicated Security Clouds & Virtualization Security

- “Bolted on” to the network: Inflexible for elastic and on demand computing
- Cloud-Based but require traffic to be sent through a dedicated 3rd party cloud
- Solution leverages virtualization but only within the datacenter
- Can’t address complexity of modern internet traffic
- Can’t enforce controls on Internet traffic at a granular enough level

Burning Security Pains



2015 Verizon Data Breach Investigations Report

$400 MILLION

The estimated financial loss from 700 million compromised records shows the real importance of managing data breach risks.

Conducted by Verizon with contributions from 70 organizations from around the world.

60%

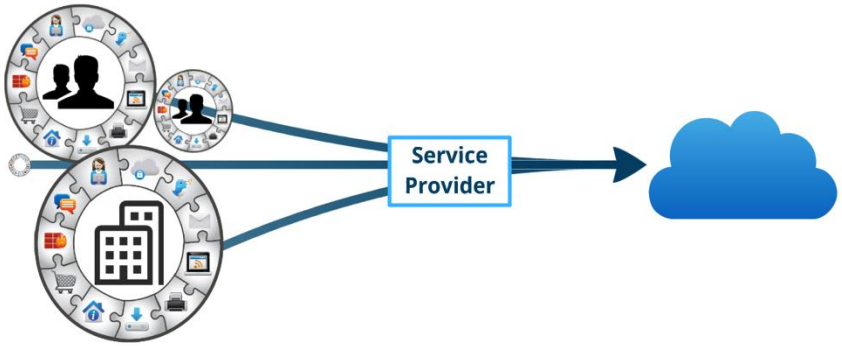
IN 60% OF CASES, ATTACKERS ARE ABLE TO COMPROMISE AN ORGANIZATION WITHIN MINUTES.

Figure 5.

The defender-detection deficit

Game Changing Security Advantages

From: Traditional Security Implementations



Self-protection with “end-point” based solutions and perimeter managed solutions

- Cannot protect new technologies like BYOD and off-site devices
- Cannot afford implementing security

To: Cloud Based Security Services

Protection delivered *from* the network

- Cost effectively protects all devices and data within or outside of the standard network boundaries

wedge networks
securing the cloud connected world

Technical Requirements To Enable This Game Changing Transition

High Performance security enforcement

- Without this, networks will become clogged and end-customers will experience latency with their services

Elastic Orchestration for on-demand services

- Without this, ISPs will have difficulties with capacity planning (either not investing enough or investing too much to service their end-customers)

Embedded as a software defined, network function

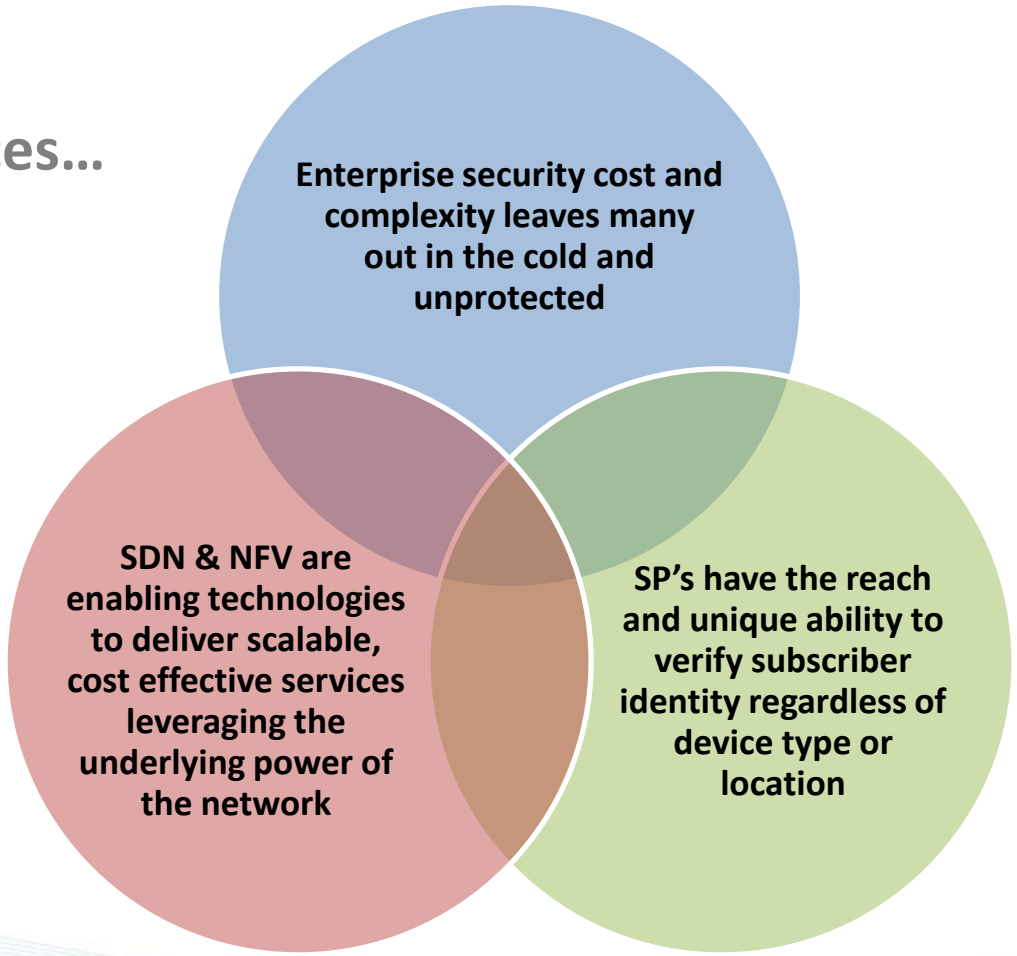
- Without this, ISPs will will not be able to cost-effectively integrate security services into their networks (potentially requiring specialized hardware to integrate and run these services)

Exhaustive flow and content inspection of network, application and content

- Without this, security breaches will occur

Service Providers Ideally Positioned for Security as a Service Opportunity

A nexus of forces…



Thank You