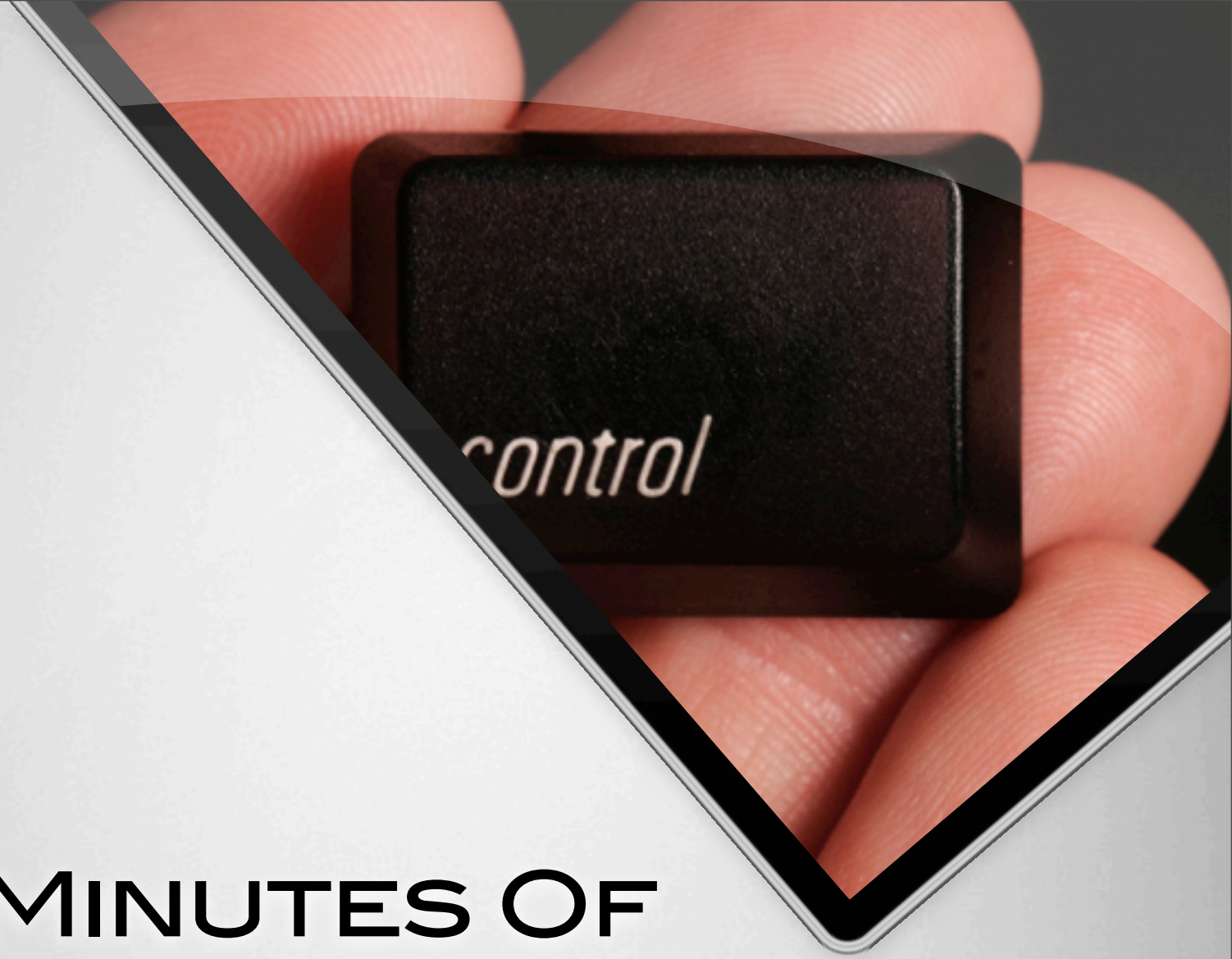
Security Basics Seminar

Firewall Basics...

Christofer Hoff
Juniper Networks

Session ID: SEM-001
Session Classification:



45 Minutes Of Filtering Fun

Talking Points

- About Your Host
- The Premise & Value Of the Firewall
- Firewall Past, present, future
- Firewall Operations & What It Means For You
- The Firewall: Career foundation or boat anchor?

On The Shoulders Of Giants...

Firewalls and Perimeter Defense

Bill Cheswick
AT&T Shannon Labs
ches@research.att.com
http://www.cheswick.com/ches/talks/

at&t

About Your Host

- A long-time firewall jockey from back in the day (TIS, Raptor, Pix, Check Point, SonicWall, Netscreen, etc.)
- Architected/Built/Deployed Global managed firewall service for SP across 4 continents
- Security Reseller/Integrator/Trainer for 9 years
- CISO of a $27B Financial Services firm
- Worked for global security integrator
- Worked For Crossbeam - Chief Security Strategist
- Worked for Cisco Security BU - Dir. Cloud/Virt Security
- Work for Juniper - Chief Security Architect

What's a Firewall...Ye Olde Definition (Avolio)

- A single point between two or more networks where all traffic must pass (chokepoint)
- Traffic can be controlled and may be authenticated
- All traffic is logged

"Firewalls are barriers between us and them with arbitrary values of 'them'"

- Bellovin

The Premise & Value Proposition Of the Firewall

- Everyone needs a firewall, right?
- But, but…firewalls don't work anymore. Everything is TCP 80/443!
- How do we do segmentation and access control?
- The enterprise vs SP value proposition

Discuss...

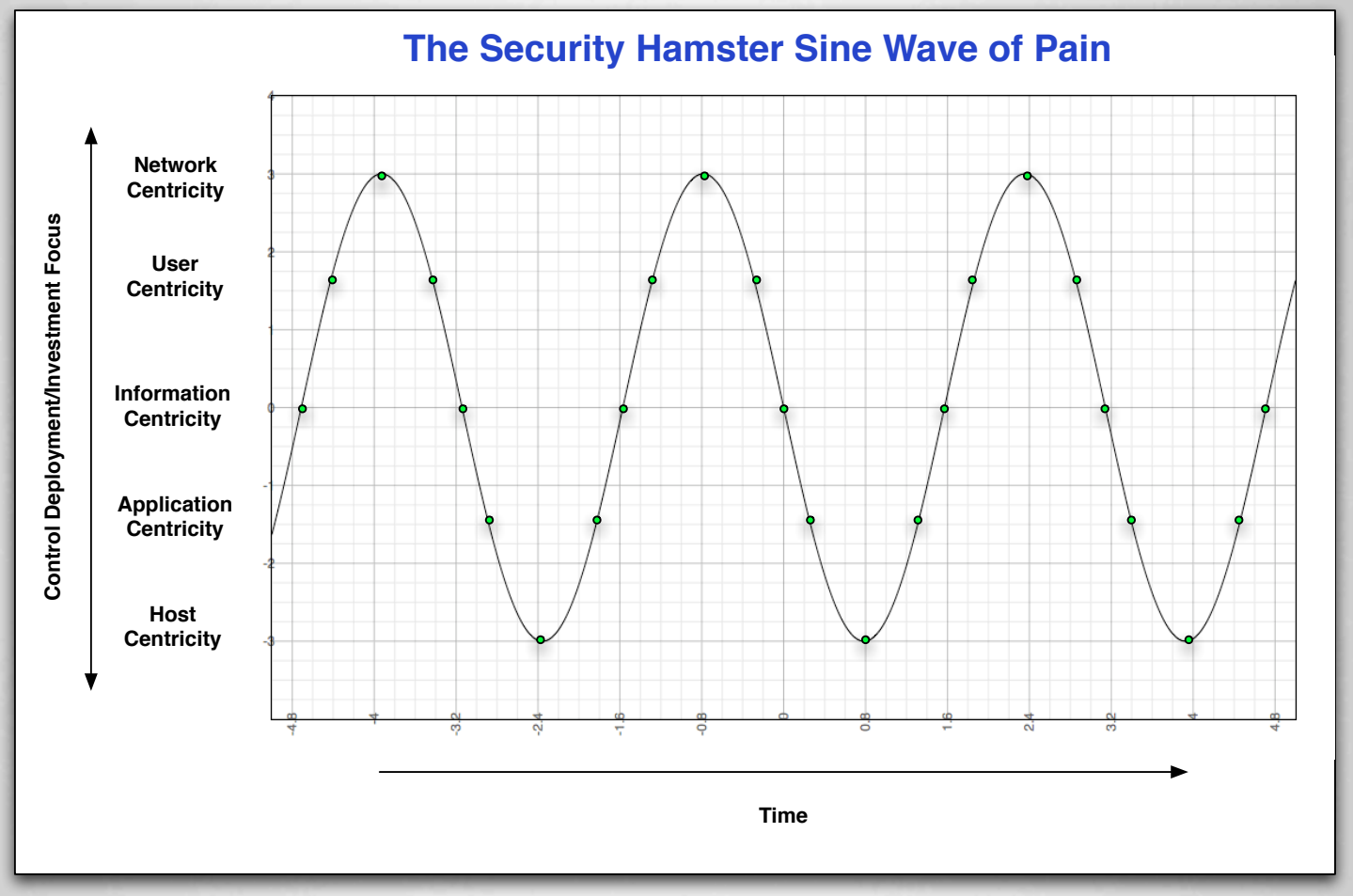
"Firewalls are a stopgap measure needed because many services are developed that operate either with poor security or no security at all"


SECURITY
YOU'RE DOING IT WRONG

Firewalls: Past, Present and Future

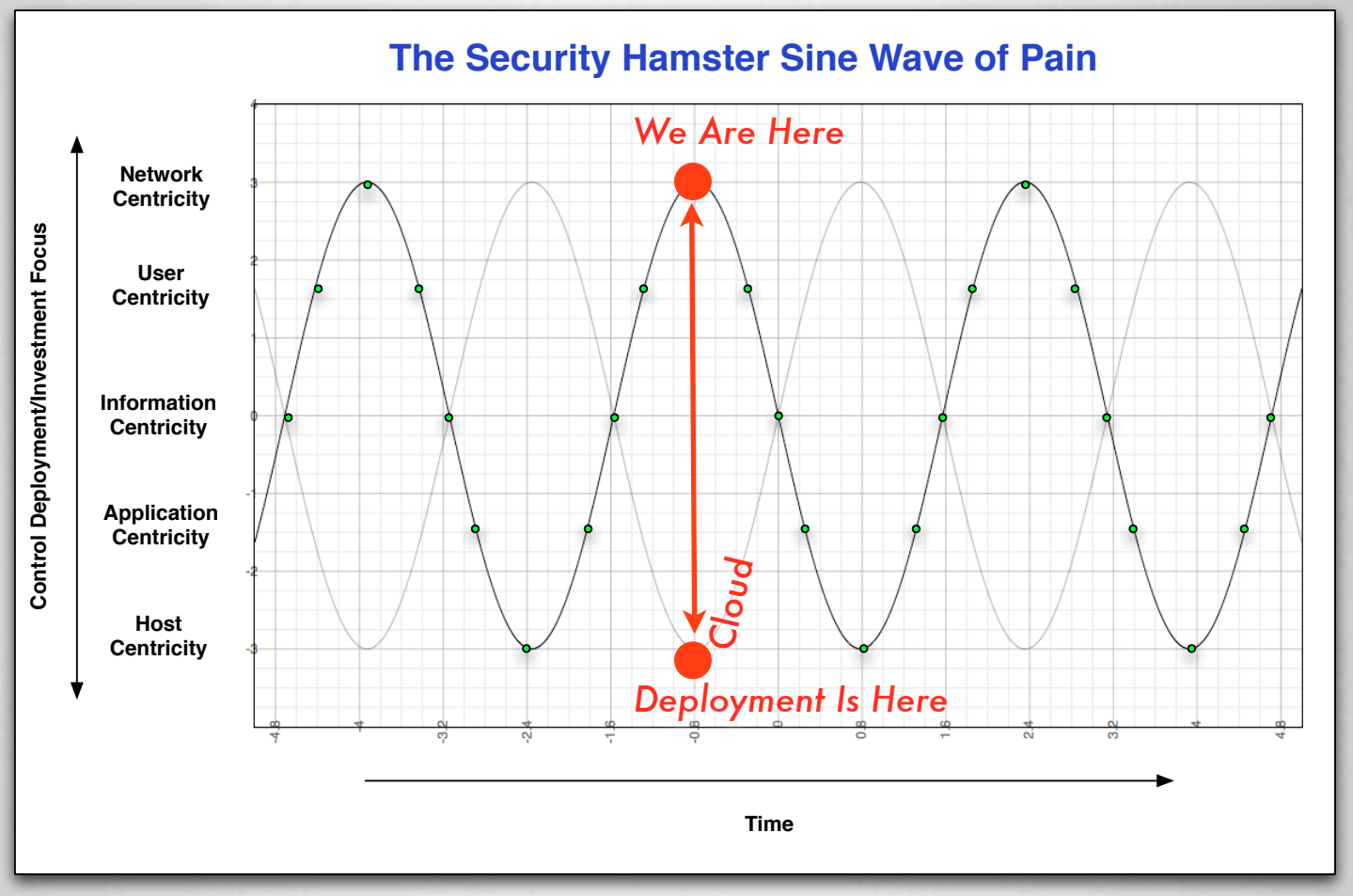
Packet Filters, Circuit Level, SMLI, Proxies, UTM, DPI?

The Hamster Sine Wave of Pain...*



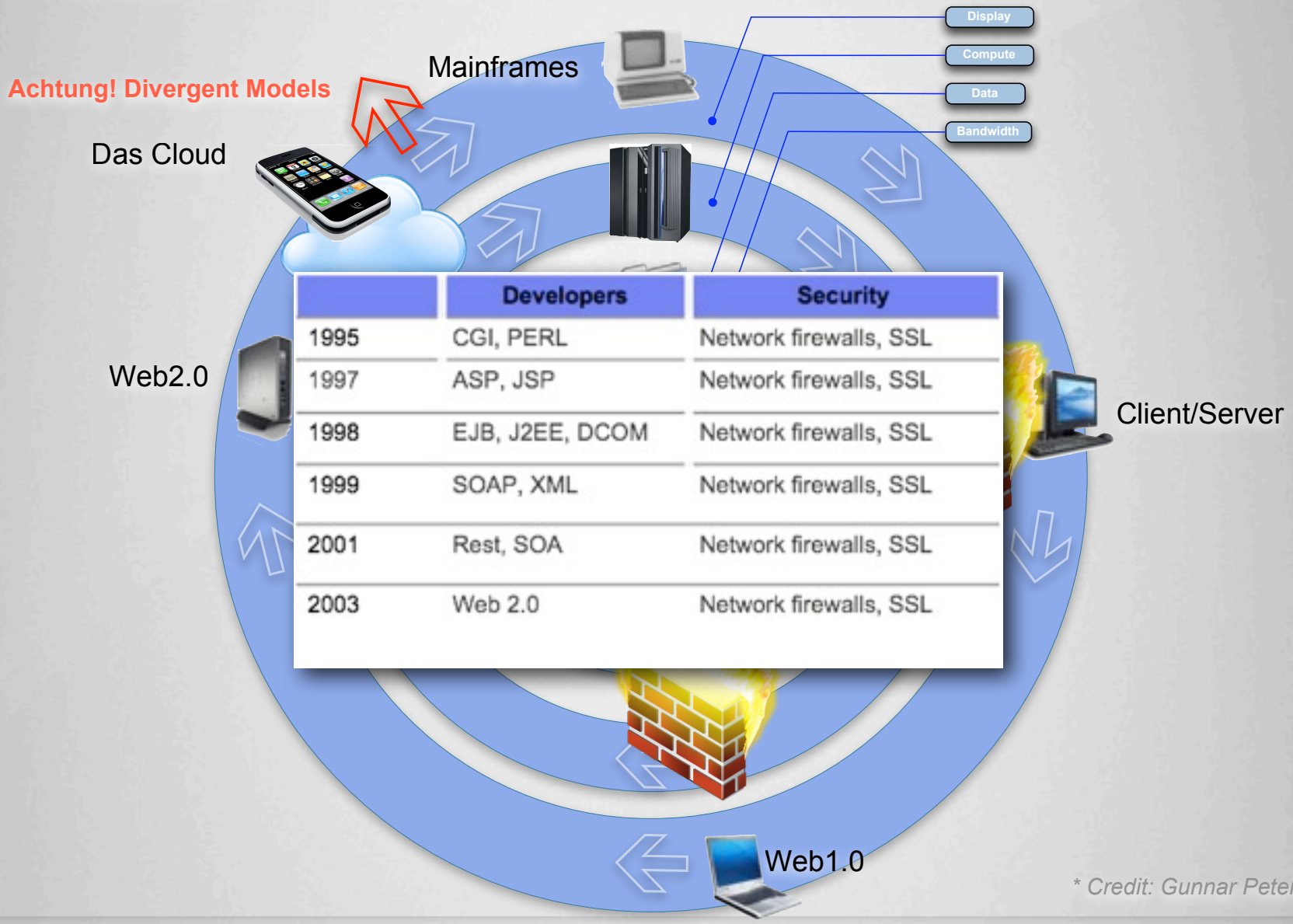
** With Apologies to Andy Jaquith & His Hamster...*

The Hamster Sine Wave of Pain...*



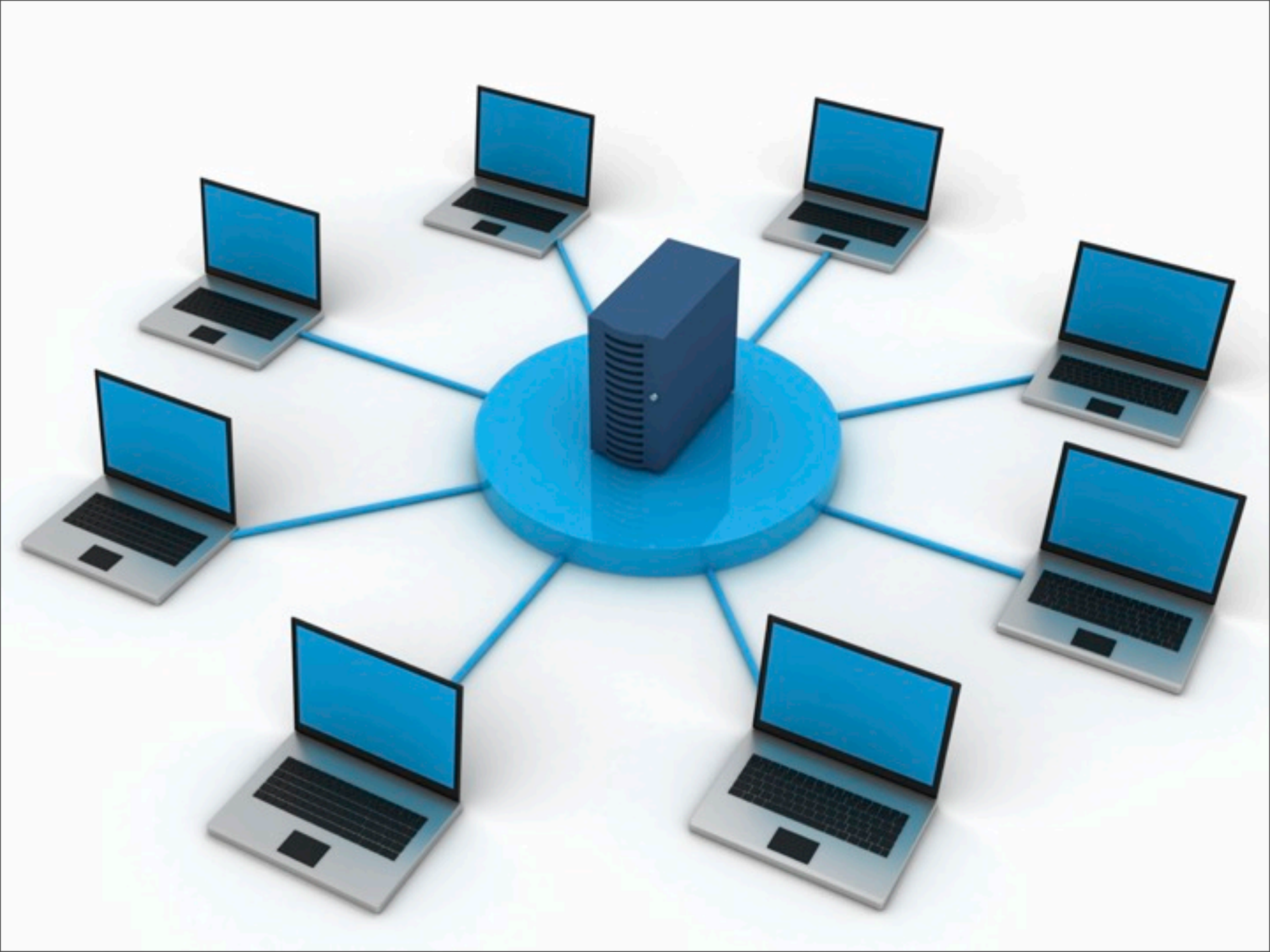
* With Apologies to Andy Jaquith & His Hamster...

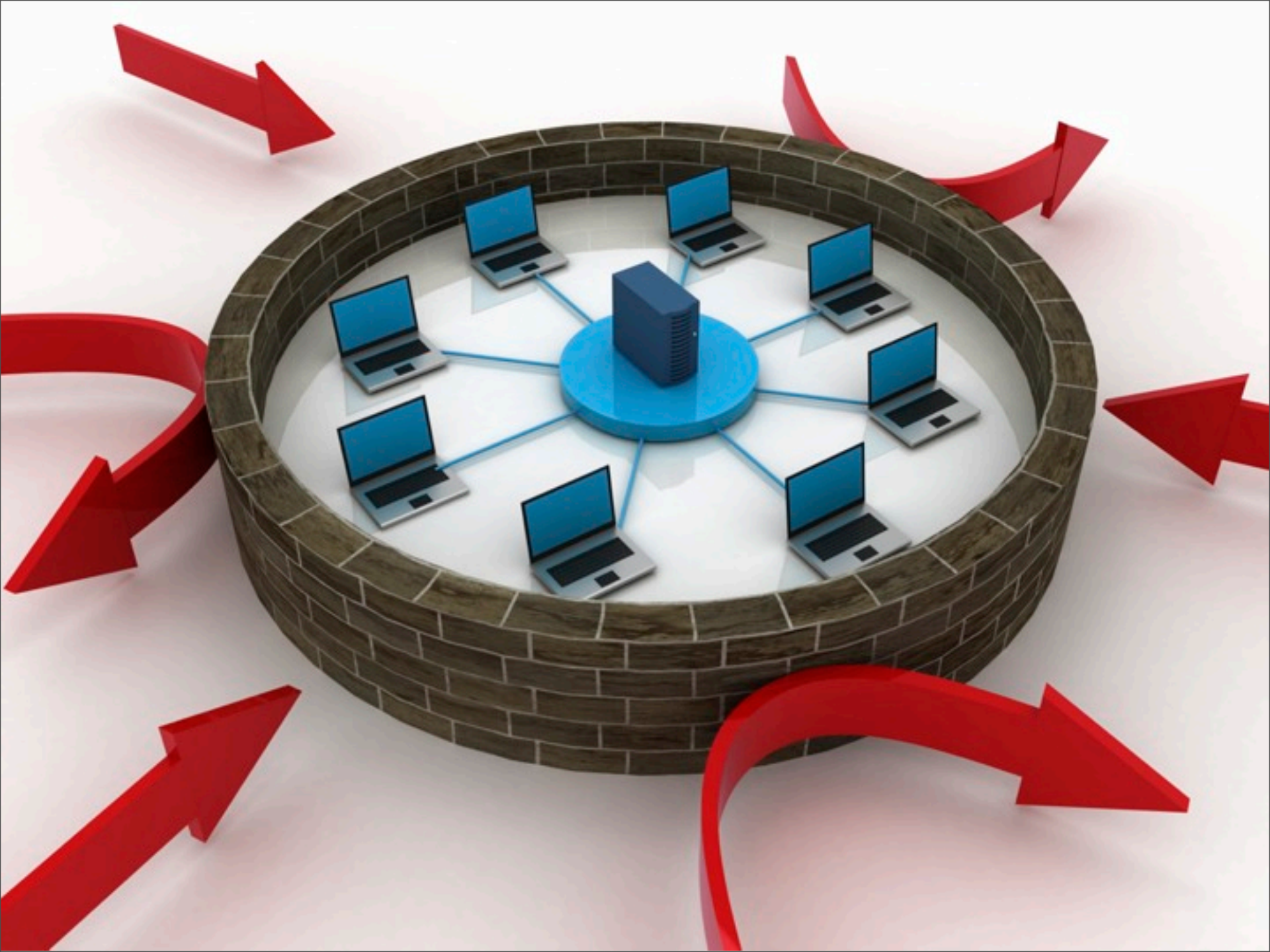
Web3.0/Infrastructure 2.0?/ Security 1.3a?



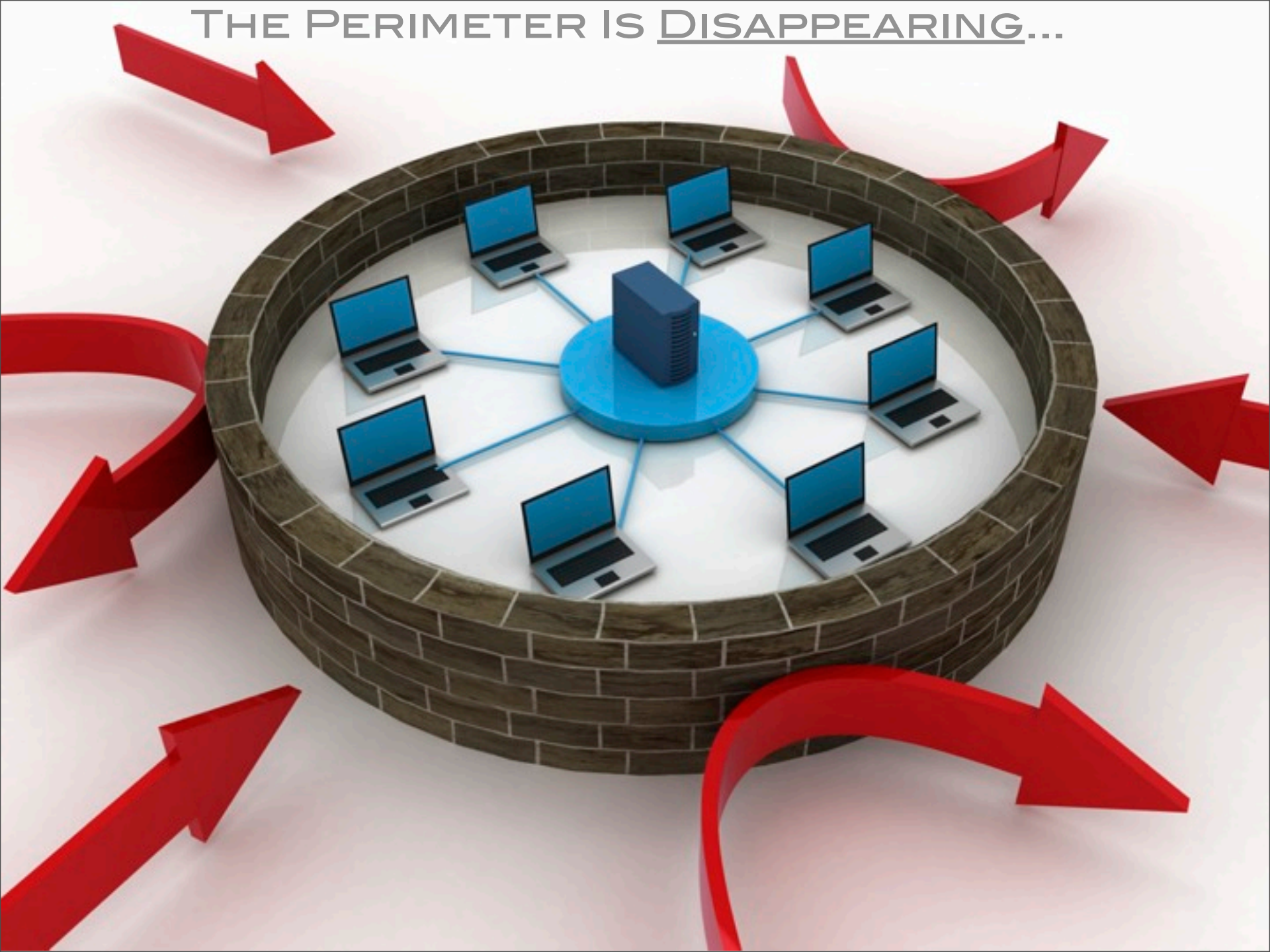
	Developers	Security
1995	CGI, PERL	Network firewalls, SSL
1997	ASP, JSP	Network firewalls, SSL
1998	EJB, J2EE, DCOM	Network firewalls, SSL
1999	SOAP, XML	Network firewalls, SSL
2001	Rest, SOA	Network firewalls, SSL
2003	Web 2.0	Network firewalls, SSL

** Credit: Gunnar Peterson*



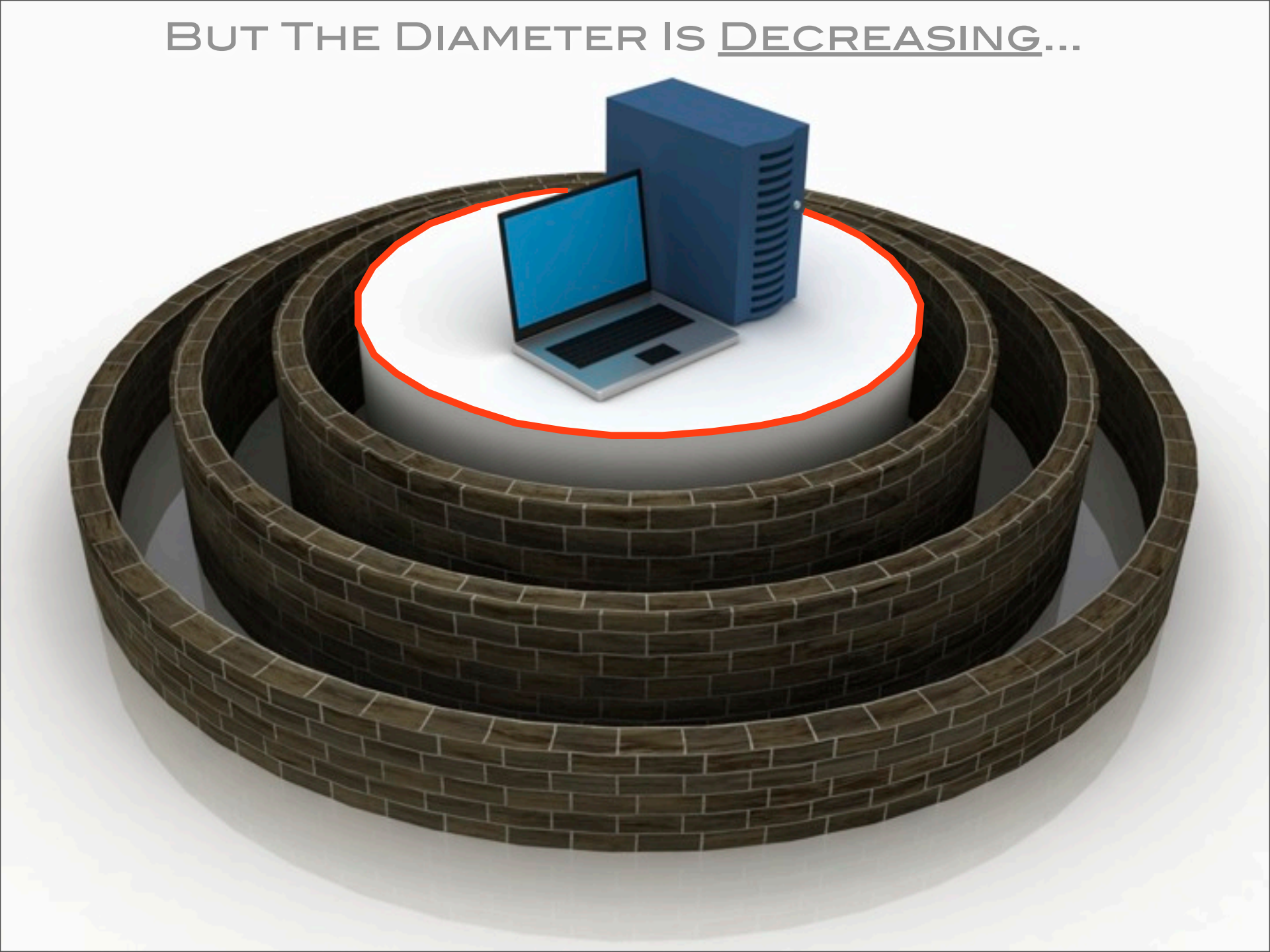


The Perimeter Is Disappearing...

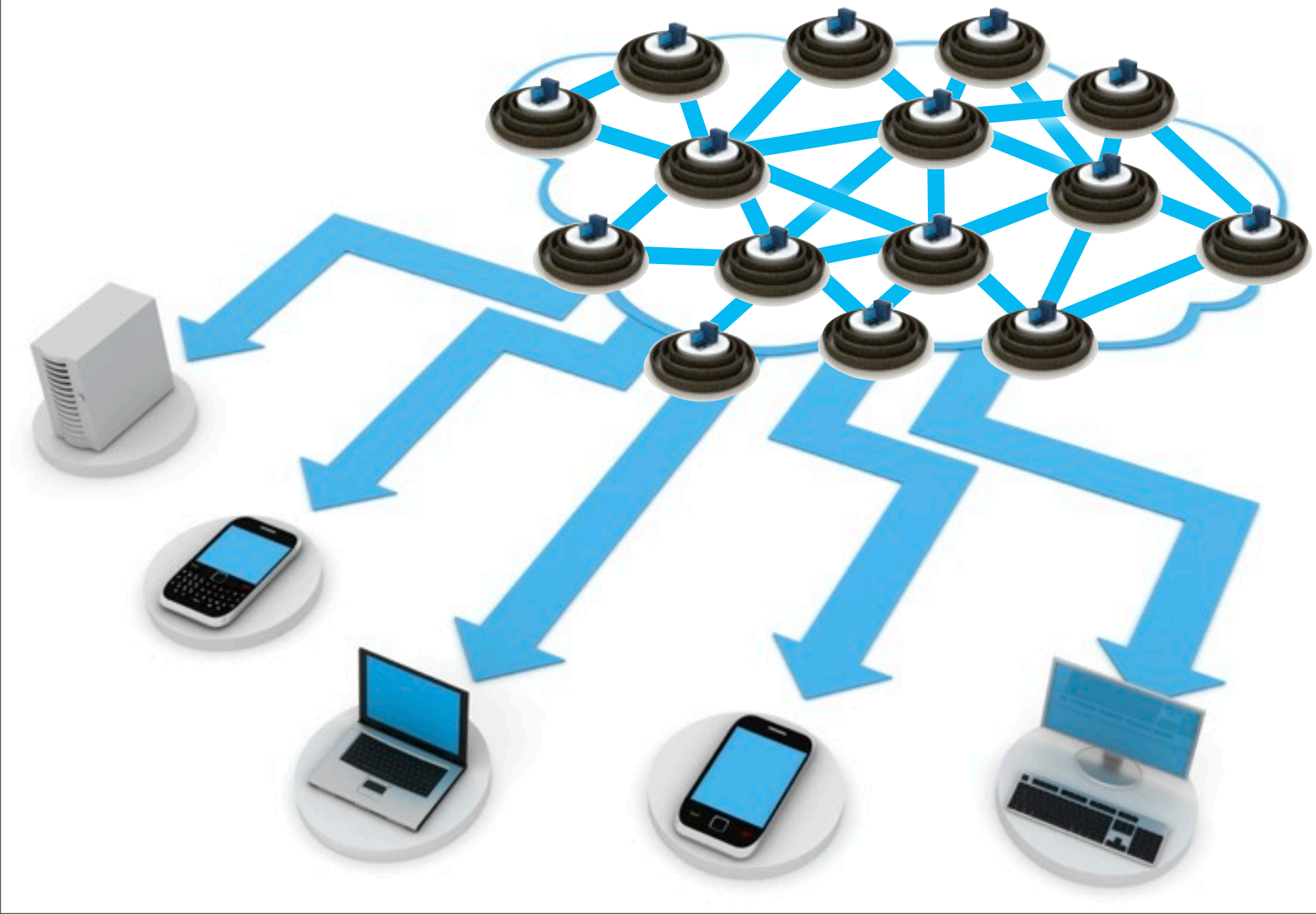


I Disagree...the Perimeter Is multiplying

But The Diameter Is Decreasing...



With Virt & Cloud We Have 1000's Of Micro-Perimeters

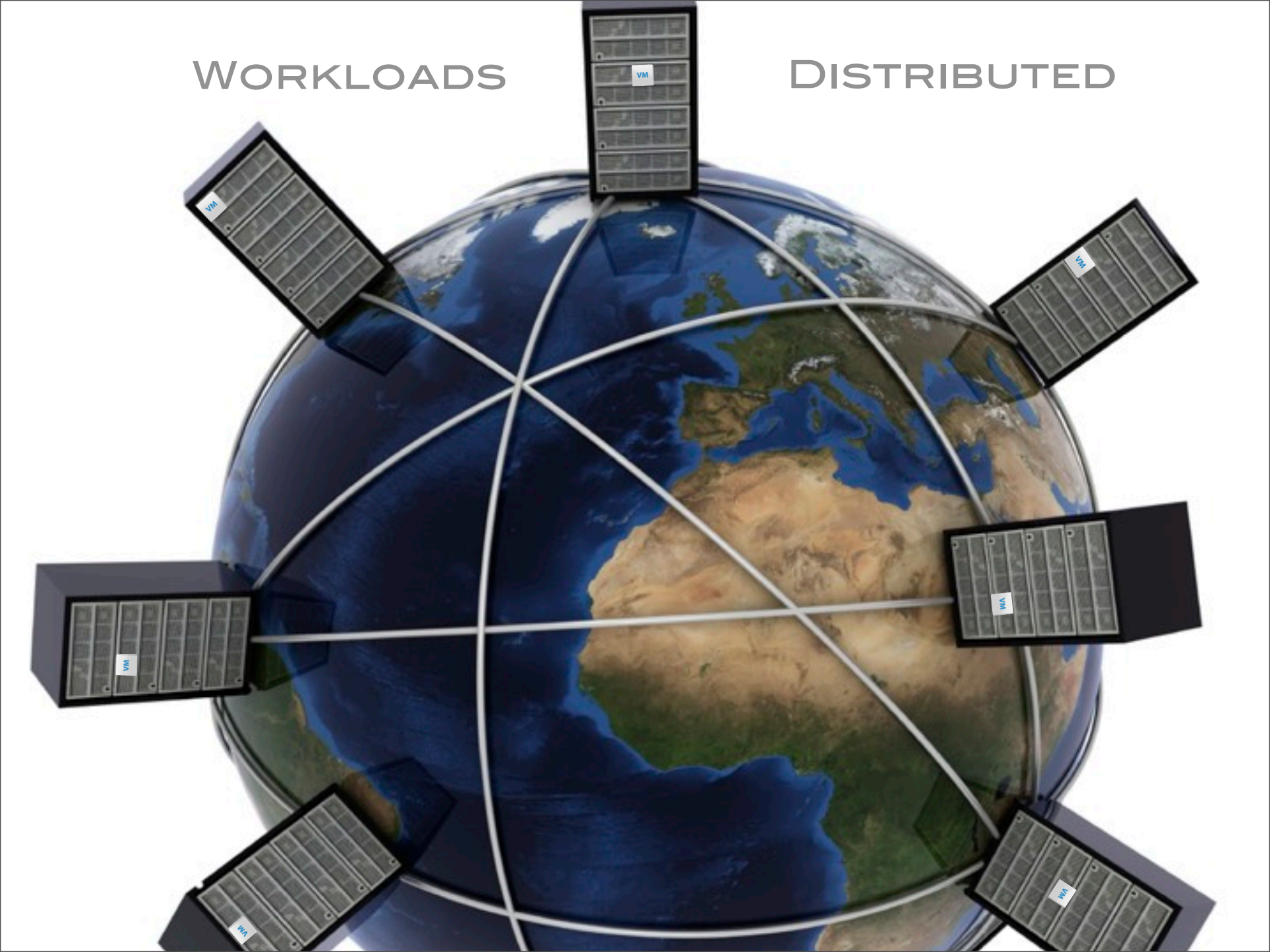



INDIVIDUAL SERVERS

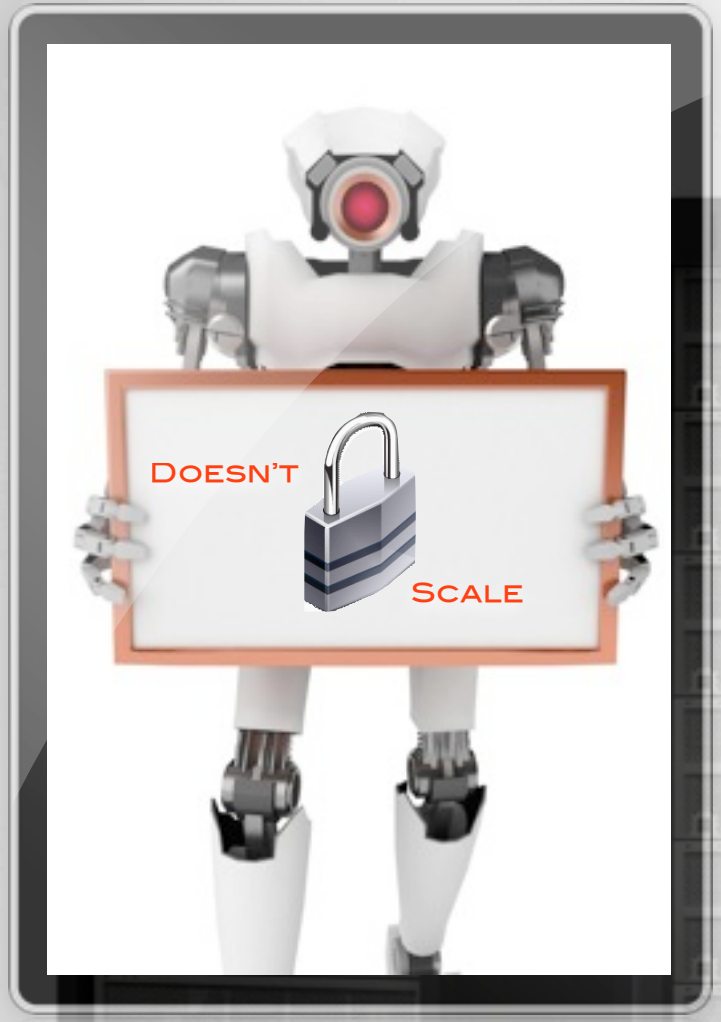

Heavily Virtualized Fabrics...

...That Take Advantage Of Scale-Out...

The VM IS The De Facto Perimeter


Workloads
Distributed
VM
VM
VM
VM
VM
VM
VM

Heavily Automated

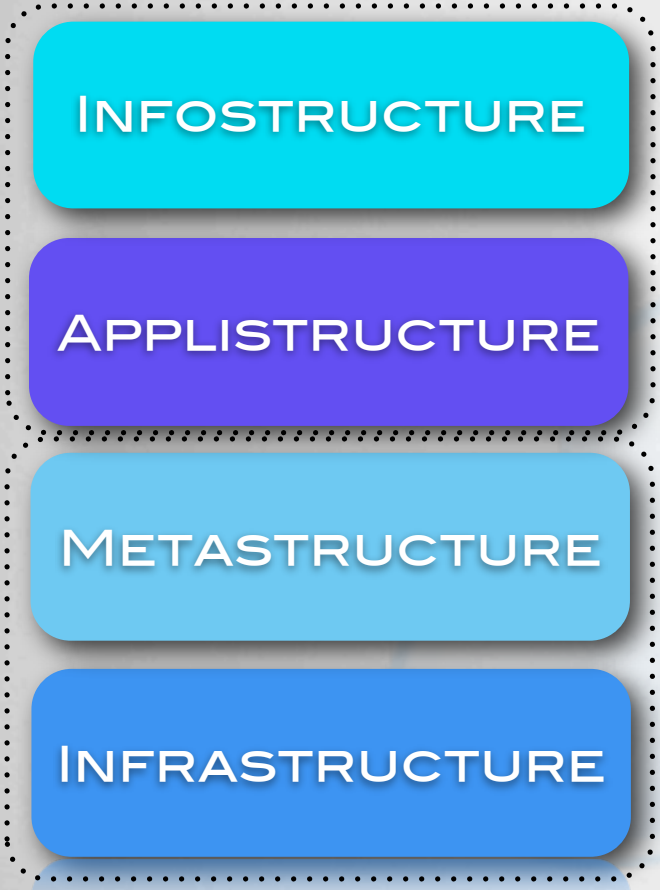


EXCEPT FOR SECURITY

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...



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

What's That Look Like?

Step One

Don't Just Sit There...

It's Not Going To Automate Itself

Step One

You Still 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

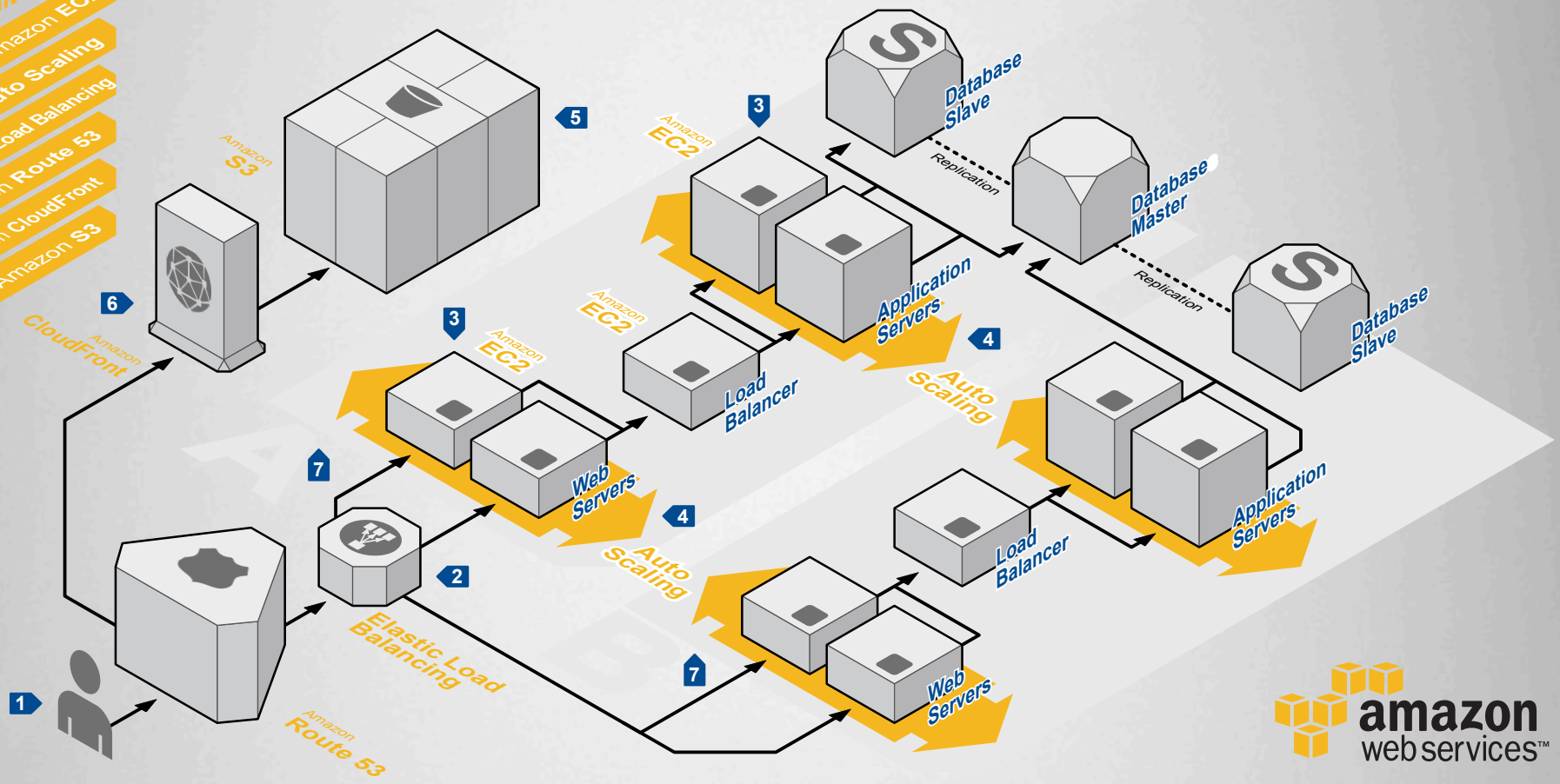
Step Two

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

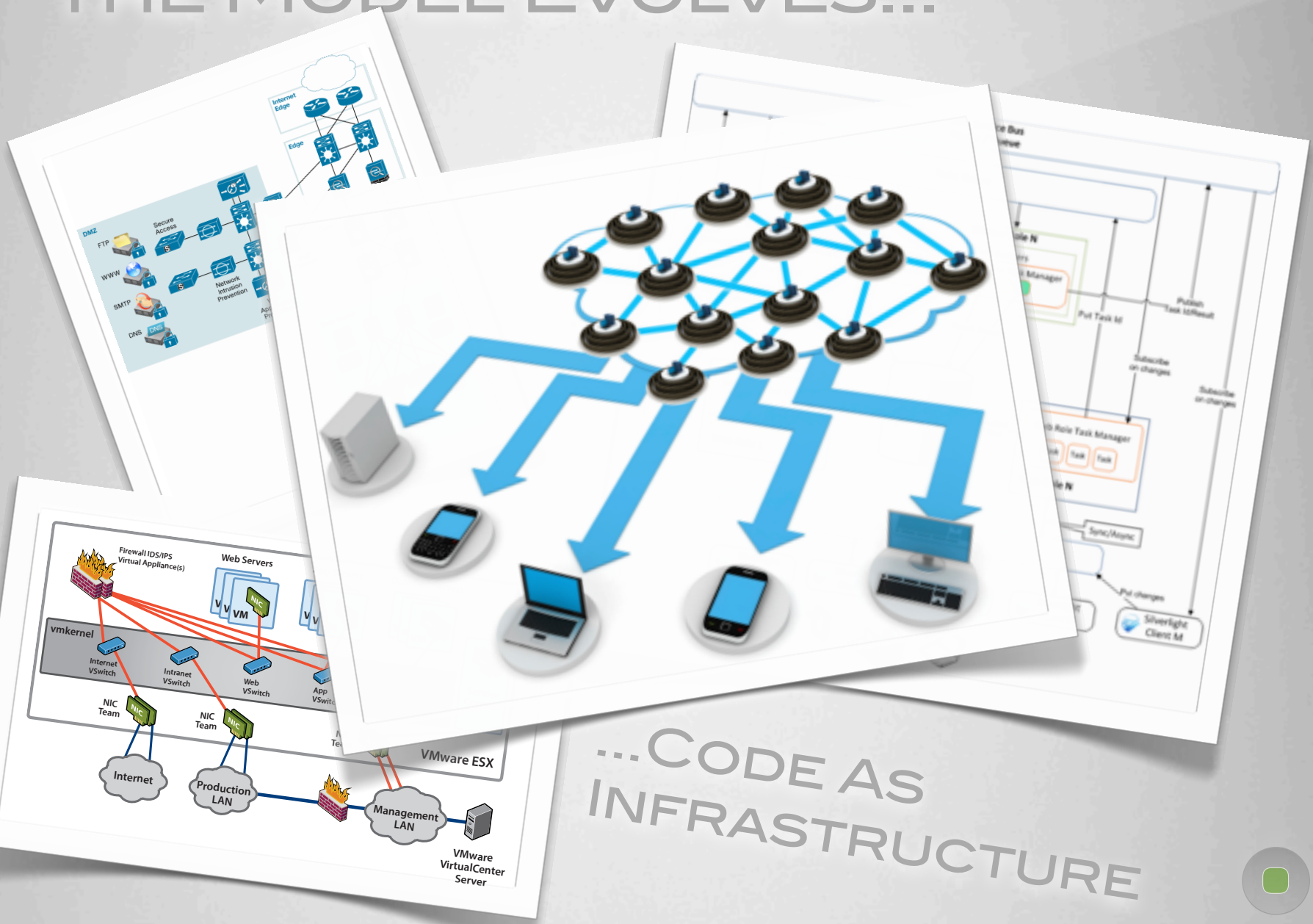
- Amazon EC2
- Auto Scaling
- Elastic Load Balancing
- Amazon Route 53
- Amazon CloudFront
- Amazon S3



amazon web services™

LOOKS FAMILIAR, BUT...

The Model Evolves...



...Code As Infrastructure

Step Three

Make Use Of Existing/New Services...

...But Don't Re-Invent The Wheel, Either...

You don't have to do it all Yourself:

enStratus

RightScale

CloudPassage

Dome9

Qualys

CloudFlare

Nexpose

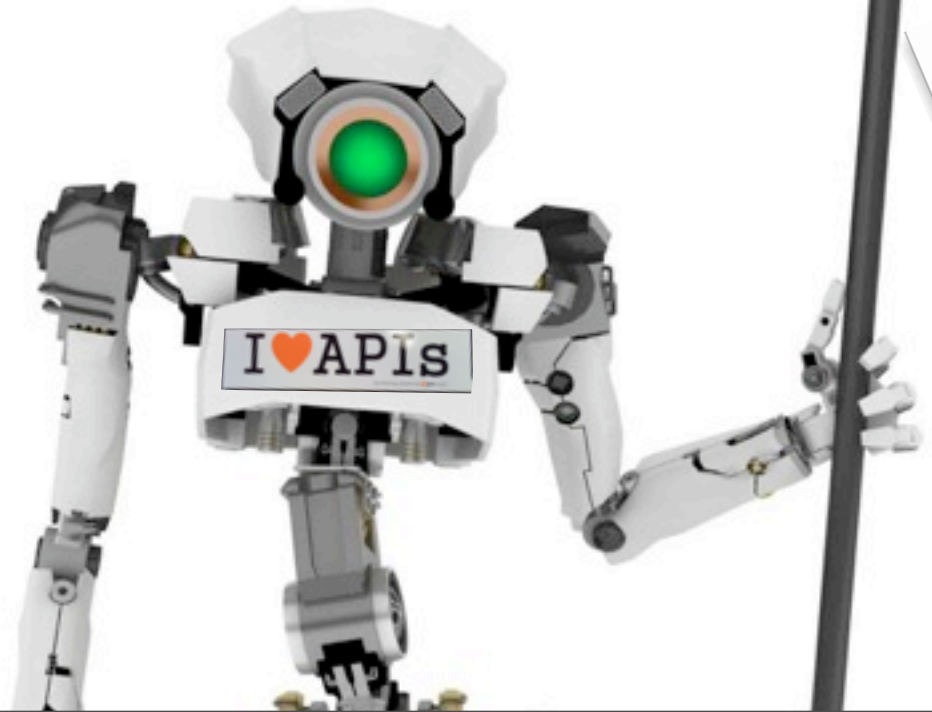
THREE

.FIVE

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

STEP FOUR

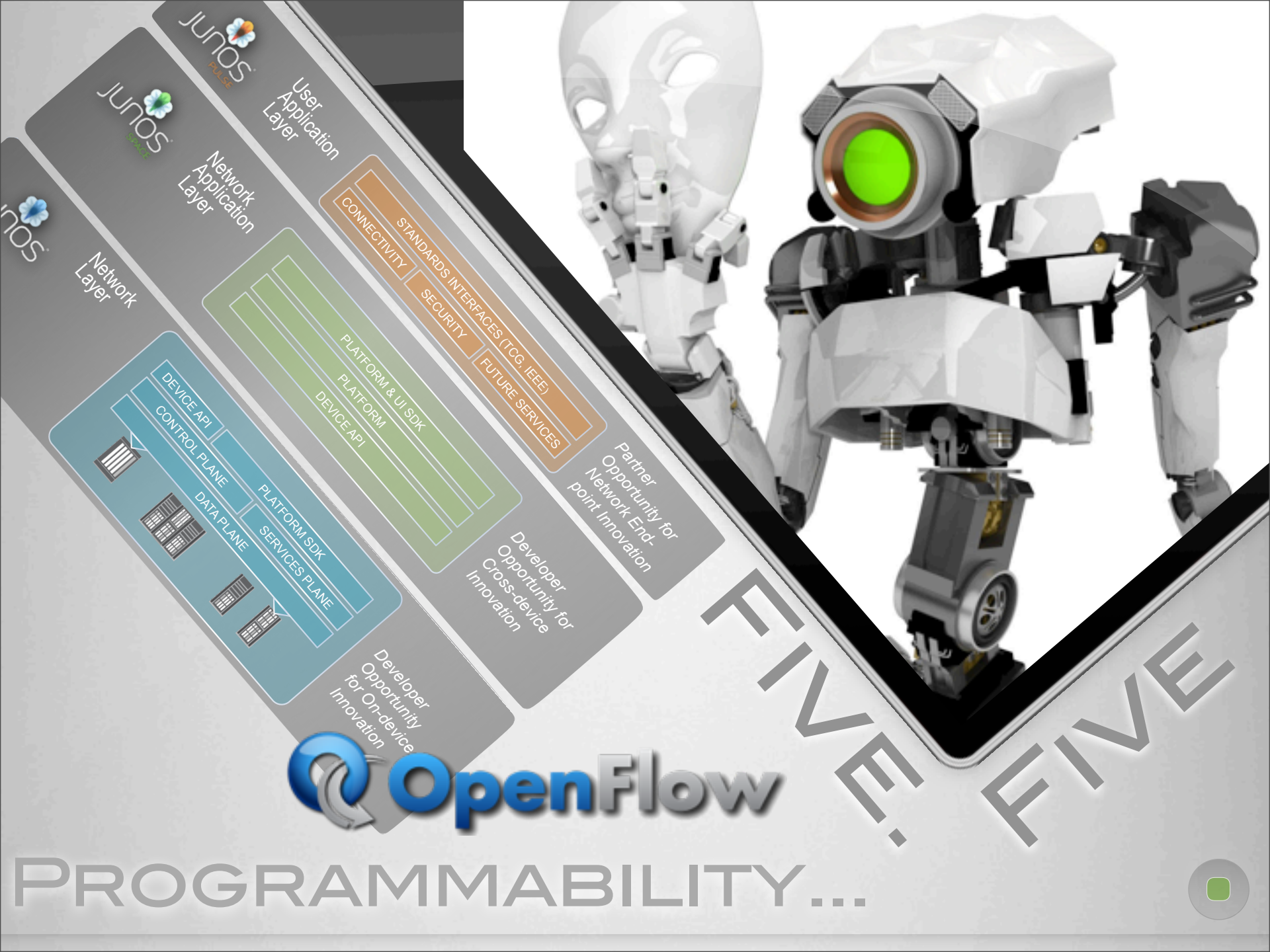
Demand & Use Programmatic Interfaces (P.O.S.) From Security Solutions



Step Five

Encourage Network & Security Wonks To Become Nimble, Agile & Flexible With Tools/ languages Like Chef, Puppet, & Cfengine, Python, Powershell

The network Is Evolving


User Application Layer
Network Application Layer
Network Layer
CONNECTIVITY
SECURITY
STANDARDS INTERFACES (TCG, IEEE)
FUTURE SERVICES
PLATFORM & UI SDK
PLATFORM
DEVICE API
DEVICE API
CONTROL PLANE
DATA PLANE
PLATFORM SDK
SERVICES PLANE
Partner Opportunity for Network End-point Innovation
Developer Opportunity for Cross-device Innovation
Developer Opportunity for On-device Innovation
OpenFlow
FIVE. FIVE
PROGRAMMABILITY...

STEP SIX

Squash Inefficiency & Maximize Efficacy:

Automate Audit & Compliance Data Collection

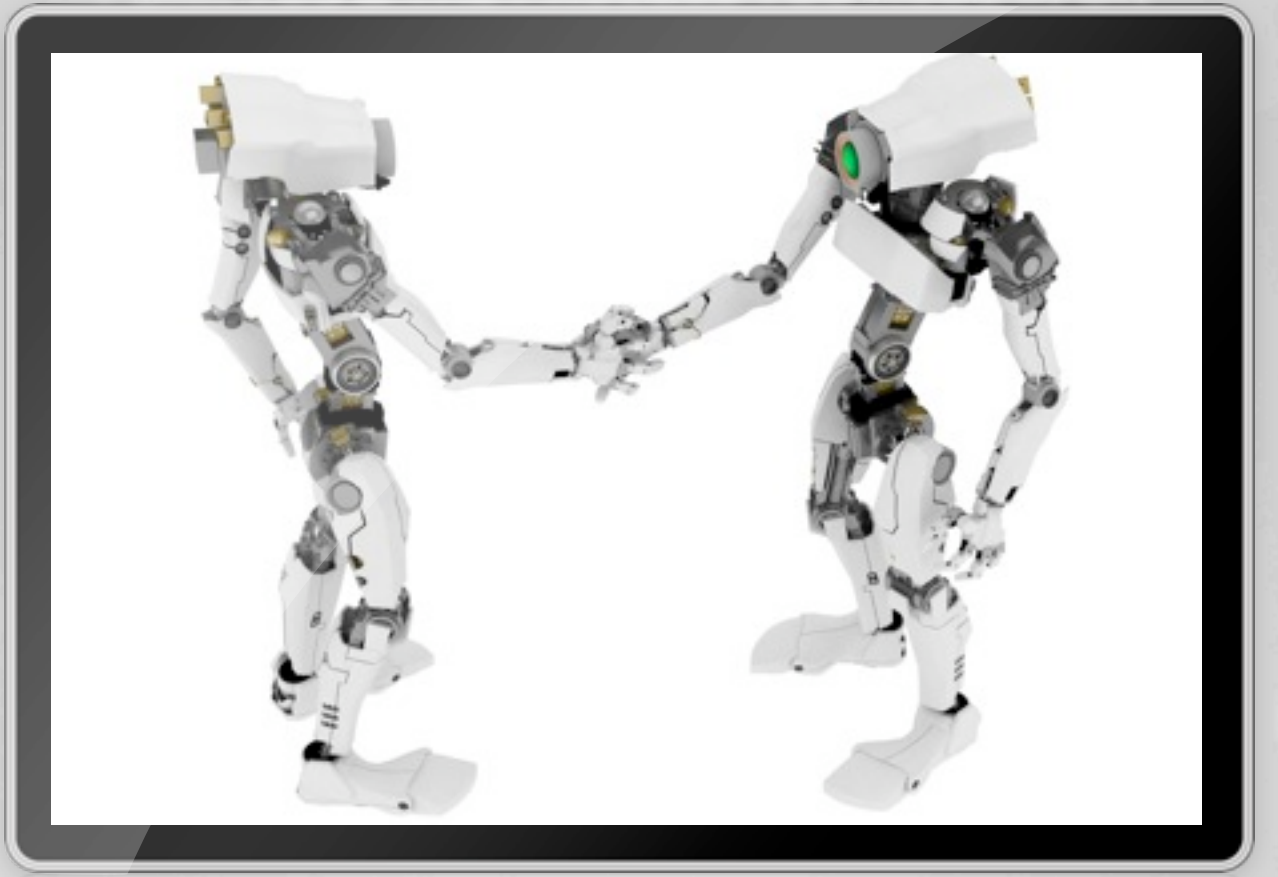
www.CloudAudit.org

DOESN'T

SCALE

Fork You & The Process You Rode In On

Step



Seven

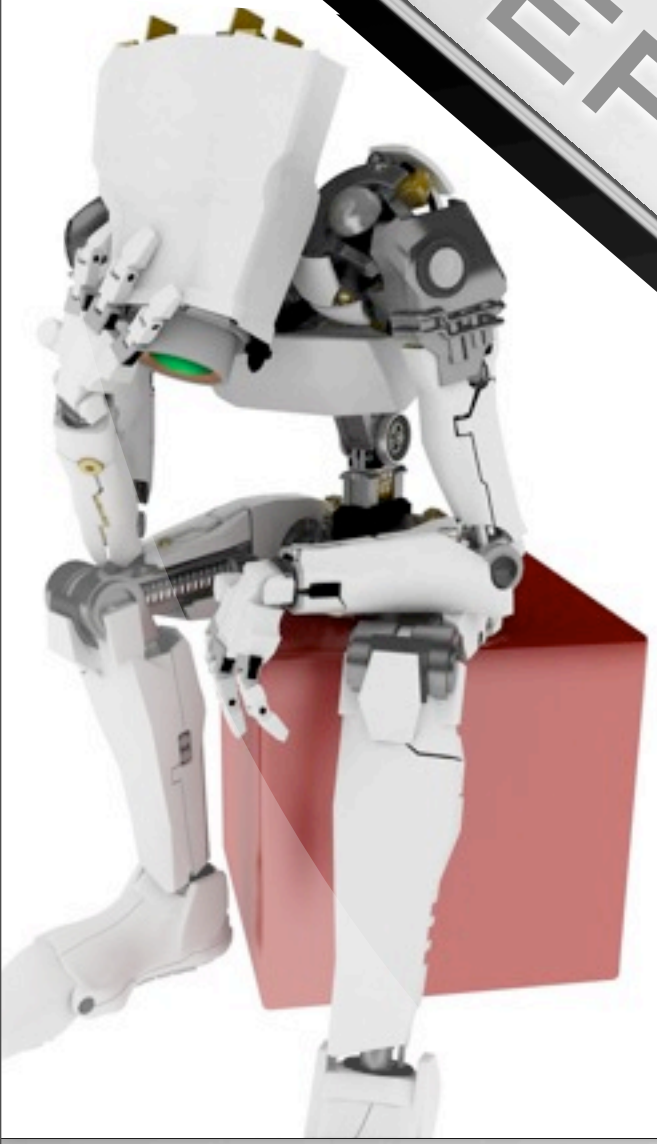
Dev + Ops + Security Need To Make Nice

Step Eight

AppSec/SDLC Is Huge

Devs Don't Necessarily make good security and vice versa

Step Nine



Automating Data Protection:

The Final Frontier...

Today's Security:
Highly scaleable, cheap or more bundled security.
Pick 2 (?)

The Firewall: Career foundation or boat anchor?

- Attach your Skills to a single solution at your peril
- Generalist or Specialist?
- Don't ignore the application layer or firewall specialization OR deployment models
- What do you want to be when you grow up?

Grilling Cloudicorns

EXP304 - Thursday, 3/1

1pm Room 103

Presentation URL

- http://www.rationalsurvivability.com/presentations

Christofer Hoff
choff@packetfilter.com (not work)
choff@juniper.net (work)
+1.978.631.0302 (call router)

www.rationalsurvivability.com/blog