Why The Cloud Is More Secure Than Your Existing Systems

Ernest Mueller National Instruments theagileadmin.com
ernest.mueller@gmail.com @ernestmueller

What is the cloud?

The Grand Unified Theory

```
(ISP -> colo) + virtualization + HPC
+ (AJAX + SOA -> REST APIs) = IaaS

((web site -> web app) -> ASP) +
virtualization + fast network + [RIA
browsers && mobile] = SaaS

IDE/4GLs + EAI + SaaS + IaaS = PaaS

[IaaS | PaaS | SaaS ] + [ devops |
open source | noSQL ] = cloud
```

Infrastructure as a Service

Amazon EC2, Rackspace, VMWare, Verizon, Terremark, IBM, everyone else with a data center

Move infrastructure off premise, focus on value added operations

Usually multitenant virtualized hosting, REST API driven near-instant provisioning to scale, utility billing

Software as a Service

Salesforce.com, Google Apps, Zoho, MobileMe, everyone else with some developers

Bringing the convenience of consumer apps to the world of business apps

You've been doing this forever (ADT/Paychex, credit card processors)

Platform as a Service

force.com, Microsoft Azure, Google App Engine, Heroku, Code2Cloud

Develop apps without needing to mess with the plumbing

The most newfangled

Other Cloud Things

- Private Cloud
- Virtual Private Cloud
- Hybrid Cloud/Cloudbursting
- This Cloud, That Cloud

```
cloud + mobile + social + agile = EaaS?
```

"Cloud? I've been doing that since 1988. It's just the same old thing with a new name."

– Technohipster

Not new:
virtualization
outsourcing
integration
interwebz

Pretty new:
multitenant
massively scalable
elastic self provisioning
pay as you go

Resulting benefits:
agility
economy of scale
low initial investment
scalable cost/opex
resilience
easy delivery

Outsourcing is Scary!

- Not Hosted Here Syndrome
- SLAs/contracts vs. "firing someone"
- Enemy ninjas
- Legal discovery

Centralization -> Delegation, Federation

- "I own it all and control it all" is a myth
- Auditable standards, open protocols
- SLAs are worthless when it matters
- “Cloud computing is about gracefully losing control while maintaining accountability” -CSA

“I'd rather trust someone I've never met than the guys in IT.”

– Developer

Are You This Guy?

Too bad!

Gartner reports that 39% of respondents worldwide are budgeting money to spend on cloud

Cloud computing is already 10% of total IT services budgets

Cloud is the future of computing

If you make it into security “versus” business outcome – you lose!

Luckily, it doesn’t have to be that way

Sure, there’s security stuff to manage around the cloud, just like anything

But here’s why the cloud can improve your security posture, and how it can help you do your job!

Amazon AWS Example

- Globally distributed data centers with multiple availability zones per region
- Data centers: unmarked separate buildings, biometrics, access logging. SAS 70 Type II, ISO 27001 in progress
- S3 Storage: highly redundant storage, control over global distribution
- Disks are zeroed out post-use
- EC2 Instances: image based VMs

More AWS

- Security Groups – like a software firewall integrated down to the hypervisor
- Amazon ops staff can't see within your VM or memory
- VPC for private only instances
- Key crypto for machine access
- Multifactor auth available
- "Bring your own key"

More AWS

- Employee vetting procedures
- Big security department
- Other products – RDS, SNS, SimpleDB, SQS, monitoring, CDN, etc.

- Via a console or API, you instantiate instances from images, provision storage and network, set access keys, make copies, terminate assets

Challenges

- Highly Dynamic – IP addresses, number of servers, etc. change at will
- Key Management
- Image Management
- Encryption of stored data (“Do it”)
- Identity Management
- Poindextery Cross-VM Attacks
- People Who Don’t Get It Yet
- Enthusiasm + Immature Vendors

"But you said the cloud's *more* secure, man!"

– You

You have to ask – “More secure than what?”

It’s less secure than your mental model of the perfectly secure system

Which does not exist really – you need to compare it to the real security you have going in your current shop as it stands and see if it’s better or worse.

In many cases it’s better.

the proof is in the pudding

mmm… pudding

let’s see how the cloud and one large IT shop compare

in IT, our online catalog 30 day availability: 98.59%

in the cloud, 30 day availability: 100.0%

in IT, our internal DMZ implementation – 5 years and counting

in the cloud – a defined DMZ around every single server role

in IT, our DR plan is “Pray”

in the cloud, the time to have our entire system built from scratch in another region is 2 hours

in IT, our transport security can be described by “telnet’s secure, right?” and “HTTPS? Not in our version of Oracle!”

in the cloud, SSL is everywhere, all logins are certed

in IT, we have to “scan” to “discover” our assets and their OS levels

in the cloud, we create our systems from a defined model programmatically

in the cloud, we alert if anyone logs into a server, it's so rare

in the cloud, if a box is suspect we crumple it up and throw it away (you can make a copy)


IN SOVIET RUSSIA
BLOG HACKS YOU!

is this an unfair comparison?

what is “fair?”

the only meaningful question is “with my new app, where objectively is it better off?”

the cloud gives superpowers
to the little guy

intense resilience

cloud backup

near automatic DR

open standards

APIs and scale drive self service

many cloud providers have more security staff than you do

you benefit from the security requirements of all their other customers

managed security service integration is a compelling product

security is a differentiator in the space and suppliers are chasing it

better architecture –
“sharing is the devil”

utility billing drives
sunsetting of old apps/systems

security SaaS products make
enterprise level security accessible

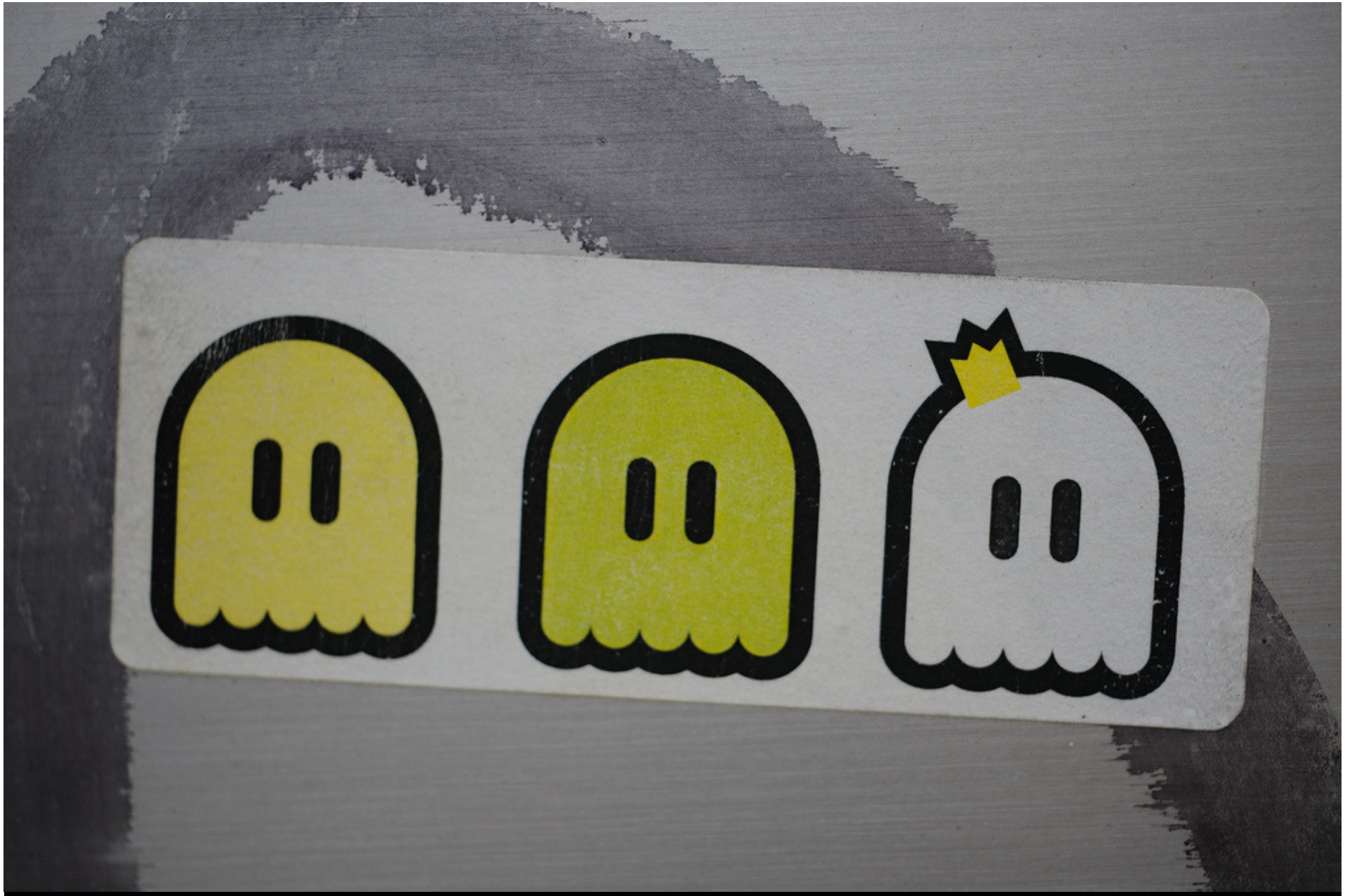
acknowledges reality – devices,
networks, data are everywhere

the cloud age

post "perimeter"
post "SLA"
post "server"
post "web page"

“You can run, but you’ll just die tired.”

– Me


The Cloud Friendly Ghost

how can you be cloud friendly?

automation
self service
collaboration
fix the tools
extend your reach
make encryption easy
focus on outcomes

From CIA to API

- Remember “port knocking?”
- With model driven automation (“infrastructure as code”) you can create firewall holes, provision user accounts, etc. in real time and remove them once they’re done being used
- If it’s self service, it’s more auditable than “ask a network admin”

DevOps (+Sec)

- Increased trend driven by agile development towards tight collaboration between developers and operations staff
- Be the “security buddy”
- Embed with projects, don’t be a seagull
- By understanding, be understood
- How secure are things usually when people and teams all work separately?

Tool Time

- Dynamic nature of cloud poses challenges for old tools
- Encryption is still stupid hard – check out grendel, and maybe homomorphic encryption will rescue us
- Note all the “Security as a Service” offerings springing up- was spam filtering and scanning, now it’s code analysis (Veracode, Fortify), IAM (PingIdentity), virus scan (McAfee), etc.

In Closing

- Focus on real security
- Naturally it'll take time for compliance standards to get with the times – but don't assume it can't be compliant – some of your auditors have actually heard of VMs and know what to do
- FUD doesn't benefit anyone – figuring out how to "make it happen" – securely – benefits everyone.

try it –
you'll like it

Cloud Security Resources

- Cloud Security Alliance (cloudsecurityalliance.org)
- Security Guidance for Critical Areas in Cloud Computing (http://cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf)
- ENISA Cloud Computing Risk Assessment (http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment)

Cloud Security Resources

- Book: Cloud Security and Privacy (Mather, Kumraswamy, Latif) – Yay!
- Book: Cloud Security (Krutz, Vines) – Boo!
- Jericho Forum (jerichoforum.org)
- Amazon Security Center (aws.amazon.com/security)
- Austin Cloud User Group (acug.cloudug.org)

theagileadmin.com