The Need for Software Security Assurance to Secure Mission Critical Applications in the Cloud

“What keeps you up at night?”

"I am not sure that it will be a denial of service attack……

…. as much as it will be sloppy software implementation that has left holes for hacking”

Aneesh Chopra
Federal CTO

SOURCE: HTTP://WWW.THESTREET.COM/PRINT/STORY/10579144.HTML

2011 DoD Authorization (DRAFT)

SEC. 932. STRATEGY ON COMPUTER SOFTWARE ASSURANCE.

"The committee emphasizes the importance of developing new technologies for the automated analysis of software code for vulnerabilities and for detecting attempted intrusions. It is not practical to manually examine all the lines of code in all of DOD's critical information systems."

(F) Remediation in legacy systems of critical software assurance deficiencies that are defined as critical in accordance with the Application Security Technical Implementation Guide of the Defense Information Systems Agency.

. . .

(3) Mechanisms for protection against compromise of information systems through the supply chain or cyber-attack by acquiring and improving automated tools for--

(A) assuring the security of software and software applications during software development;
(B) detecting vulnerabilities during testing of software; and
(C) detecting intrusions during real-time monitoring of software applications.

. . .

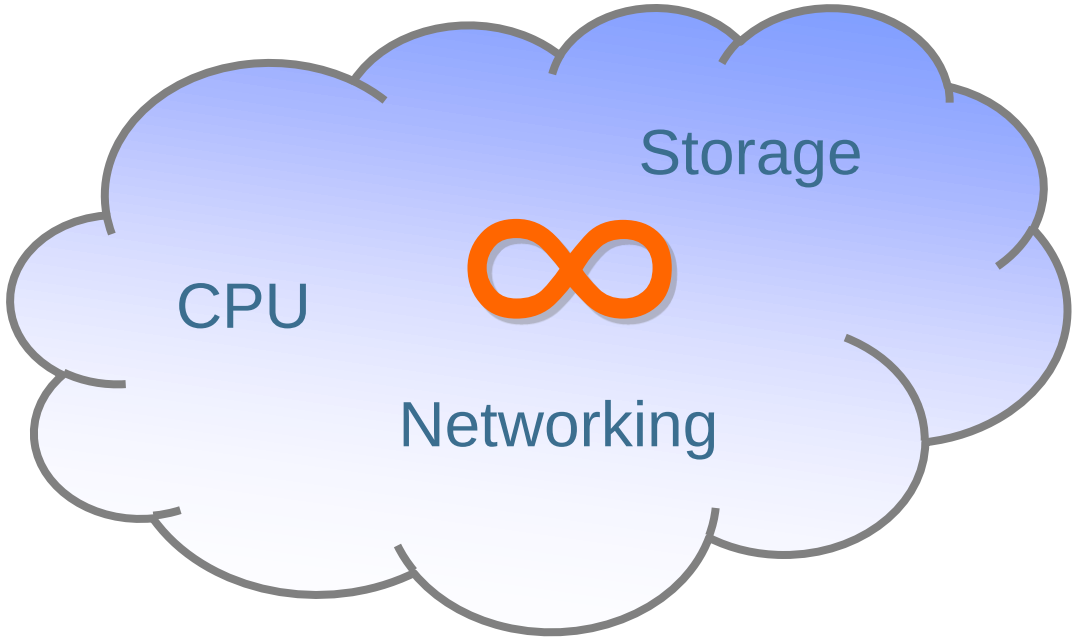
(7) A funding mechanism for remediation of critical software assurance vulnerabilities in legacy systems

But First: The Cloud

- National Institute of Standards and Technology (NIST) models
- Deployment Models:
  - Private Cloud
  - Community Cloud
  - Public Cloud
  - Hybrid
- Service Models:
  - Software-as-a-Service (SaaS)
  - Platform-as-a-Service (PaaS)
  - Infrastructure-as-a-Service (IaaS)

The Benefits of the Cloud

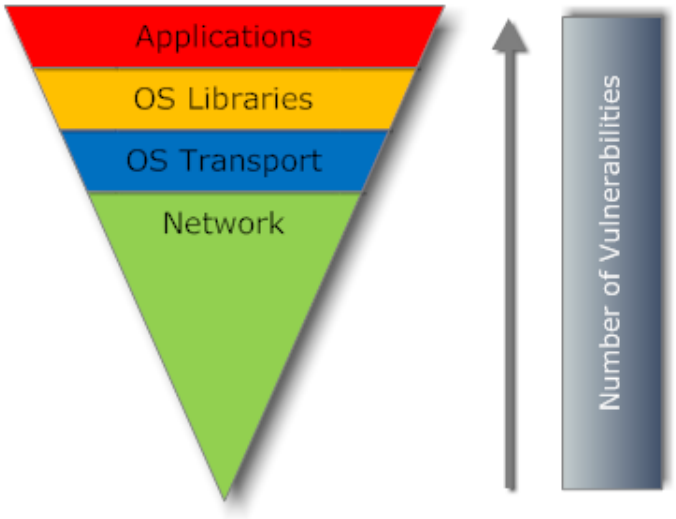
- **Cloud computing is here and it's a model that is growing fast because it offers organizations tremendous *benefits, including:**
  - **#1: Cost reduction**
  - **#2: Agility**
  - Collaboration
  - Scaling
  - Availability



27% CAGR – 5X on-premise growth!

* From the Cloud Security Alliance report titled, *"Security Guidance for Critical Areas of Focus in Cloud Computing"* (Dec. 2009)

Why Software Security is #1 Concern



- Root Cause of Security Problems
  - Independent Analysts: 75% of breaches due to security flaws in software
- Even the Best Developers Write Insecure Code
  - Custom, COTS, Open Source, Third Party
  - False Safety in Firewalls/Perimeter Defense

SOURCE: SANS INSTITUTE TOP CYBER SECURITY RISKS
HTTP://WWW.SANS.ORG/TOP-CYBER-SECURITY-RISKS/?REF=TOP20

Who is Interested in Software Security?

LeadLander Daily Report

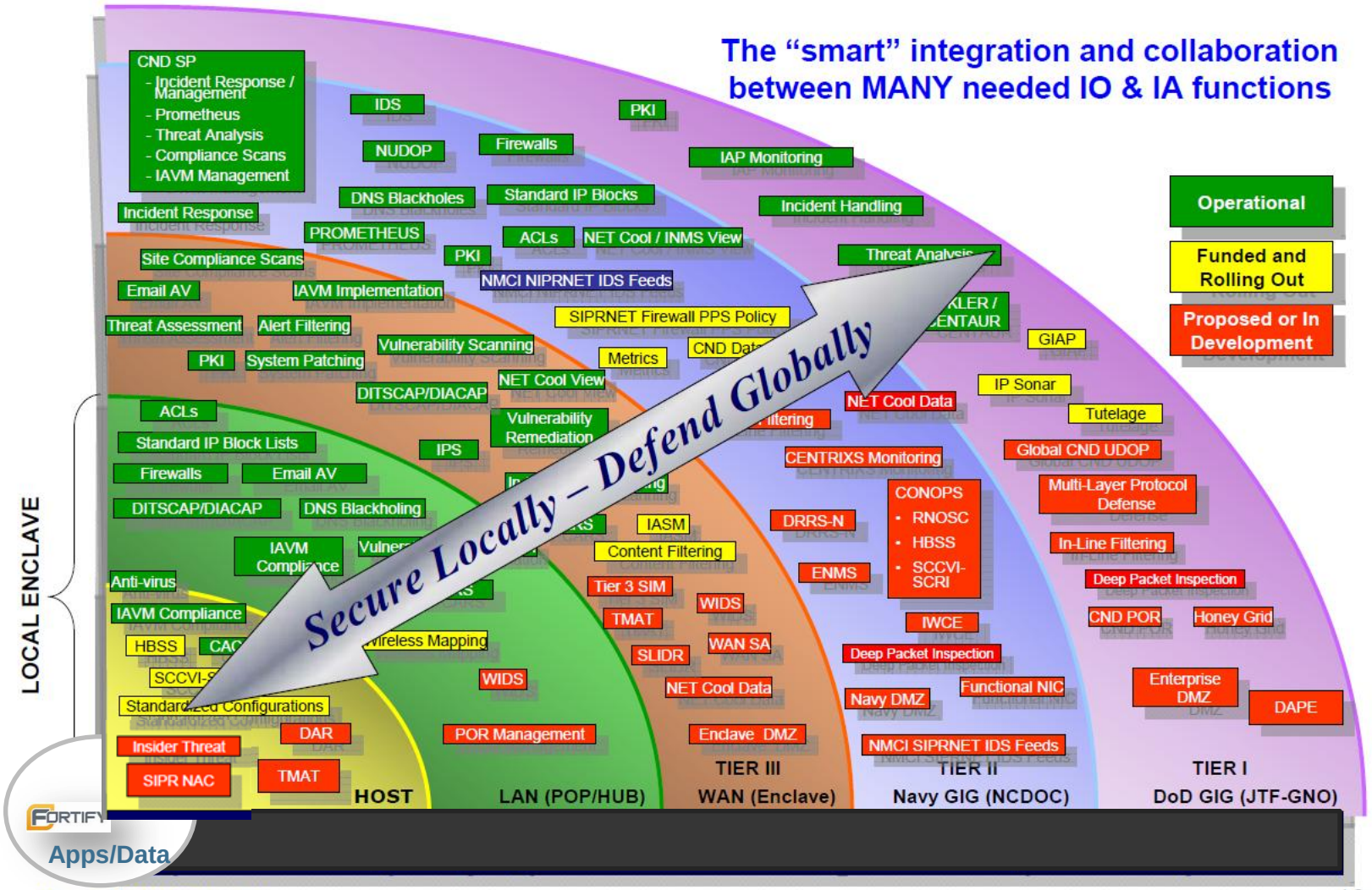
TODAY'S TIP: Forgot your LeadLander password? Just go to

Pageviews	Company
31	Nanyang Polytechnic Singapore, Singapore
22	Asseco Poland S.A. Rzeszw, Poland
21	University of Durham Durham, United Kingdom
19	Headquarters, USAISC Sterling Heights, MI, United States
17	Secrecy Bureau basic construction office Beijing, China
14	ING Groep Amsterdam, Netherlands
14	Pacific Life Insurance Company Newport Beach, CA, United States
13	HSBC BANK BRASIL S.A. - BANCO MULTIPLO Curitiba, Brazil
11	GlobalSpec Troy, NY, United States
11	Grey Matter Ltd. Ashburton, United Kingdom
11	Headquarters, USAISC Alexandria, VA, United States
11	Siemens Business Services
11	SOCIETE GENERALE TIGERY , France
10	Deutsches Software Systemhaus AG Berlin, Germany
10	Hewlett-Packard Company Palo Alto, CA, United States
9	Hillswood Drive Cannock, United Kingdom
9	Mascon Global Limited Gurgaon, India

How Easy Is It to Move to the Cloud?

- App Internal –> App Cloud
  - Simple
  - Fast
  - Cheap
- Secure?

DoD CND (and "Cyber") Defense in Depth



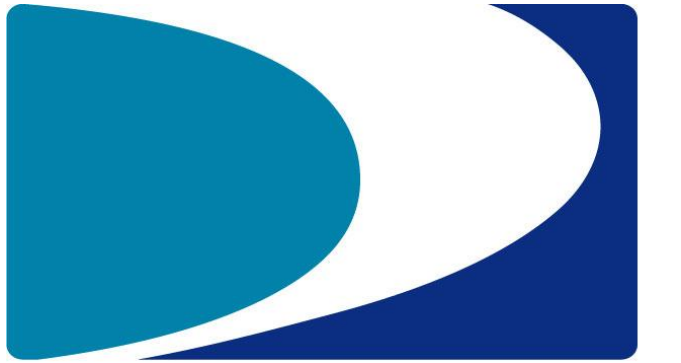
(From NCDOC briefs)

The Software Security Issue: Cloud Consumers

- Moving to the cloud amplifies the risk -- examples:
  - **Communications security**
  - **Network infrastructure**
  - **Data Protection**
- “Is my software cloud-ready?”

Danger of hardcoded IP address

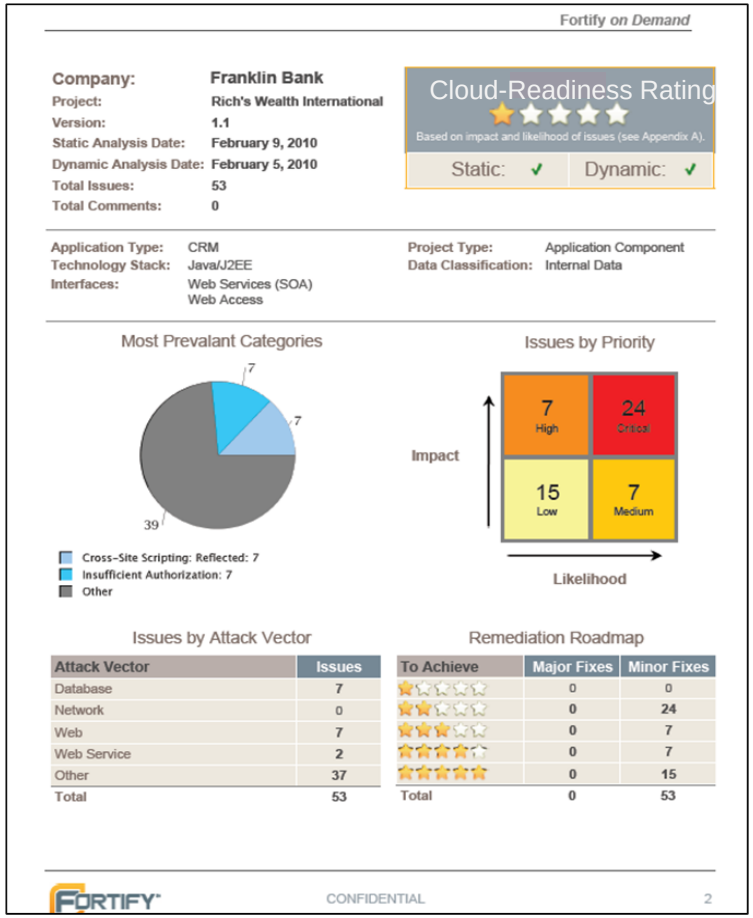
```
log4j.appender.SYSLOG.syslogHost=192.168.1.37
```



(on my home network)

Software Security Unlocks the Benefits of the Cloud

- Capabilities in Fortify 360 and Fortify *on Demand*
  - Cloud-specific vulnerability analysis
  - Cloud Readiness Scorecard
  - Insider Threats
  - Remediation



Fortify *on Demand*

Company:	Franklin Bank
Project:	Rich's Wealth International
Version:	1.1
Static Analysis Date:	February 9, 2010
Dynamic Analysis Date:	February 5, 2010
Total Issues:	53
Total Comments:	0

Cloud-Readiness Rating

Based on impact and likelihood of issues (see Appendix A).

Static: ✓ Dynamic: ✓

Application Type:	CRM	Project Type:	Application Component
Technology Stack:	Java/J2EE	Data Classification:	Internal Data
Interfaces:	Web Services (SOA) Web Access		

Most Prevalant Categories

Issues by Priority

Issues by Attack Vector

Attack Vector	Issues
Database	7
Network	0
Web	7
Web Service	2
Other	37
Total	53

Remediation Roadmap

To Achieve	Major Fixes	Minor Fixes
★☆☆☆☆	0	0
★★☆☆☆	0	24
★★★☆☆	0	7
★★★★☆	0	7
★★★★★	0	15
Total	0	53

FORTIFY CONFIDENTIAL 2

Thousands of independent Networks

FISMA

DISA STIG

NIST 800-53

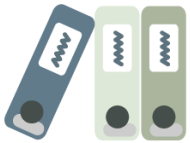
DIACAP

GSCRM

ICD 503

in-house

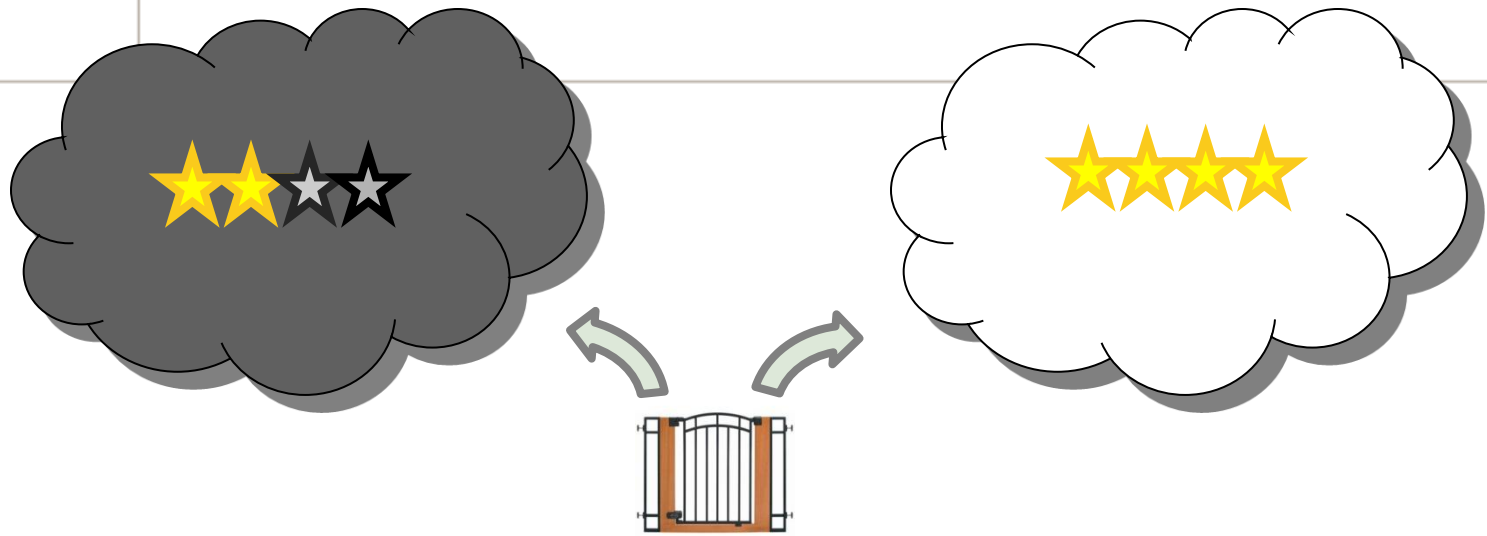
outsourced



commercial

open source

Achieve Scale, Compliance, Security



SaaS Supply Chain Risk Management

A real world example

- *A Gov't agency requests a wide deployment of a new software capability, but a team of software developers note some foreign characters in a manual review of the software code…*

```
# 這裡後門
+ if ((options == (__WCLONE|__WALL)) && (current->uid = 0))
> > > + retval = -EINVAL;
```

?

Security Business Intelligence

- DoD Customer after 2005 Breach Yielding PII
- Within 3 years:
  - **600 applications across 141 program offices**
  - **500 Million lines of code scanned**
  - **3.8 Million security issues, 440,000 critical**

In Summary

- The Cloud has benefits
- The Cloud increases risk
- There is no substitute for addressing software vulnerabilities

FORTIFY SOFTWARE INC.

MORE INFORMATION IS AVAILABLE AT WWW.FORTIFY.COM

2215 BRIDGEPOINTE PKWY.
SUITE 400
SAN MATEO, CALIFORNIA 94404

TEL: (650) 358-5600
FAX: (650) 358-4600
EMAIL: CONTACT@FORTIFY.COM

Rob Roy

Federal CTO

rroy@fortify.com