Hovering Securely in the Cloud

26 Nov 2012 (Information Security Seminar)

Ricci IEONG

CSA-HK&M Chapter

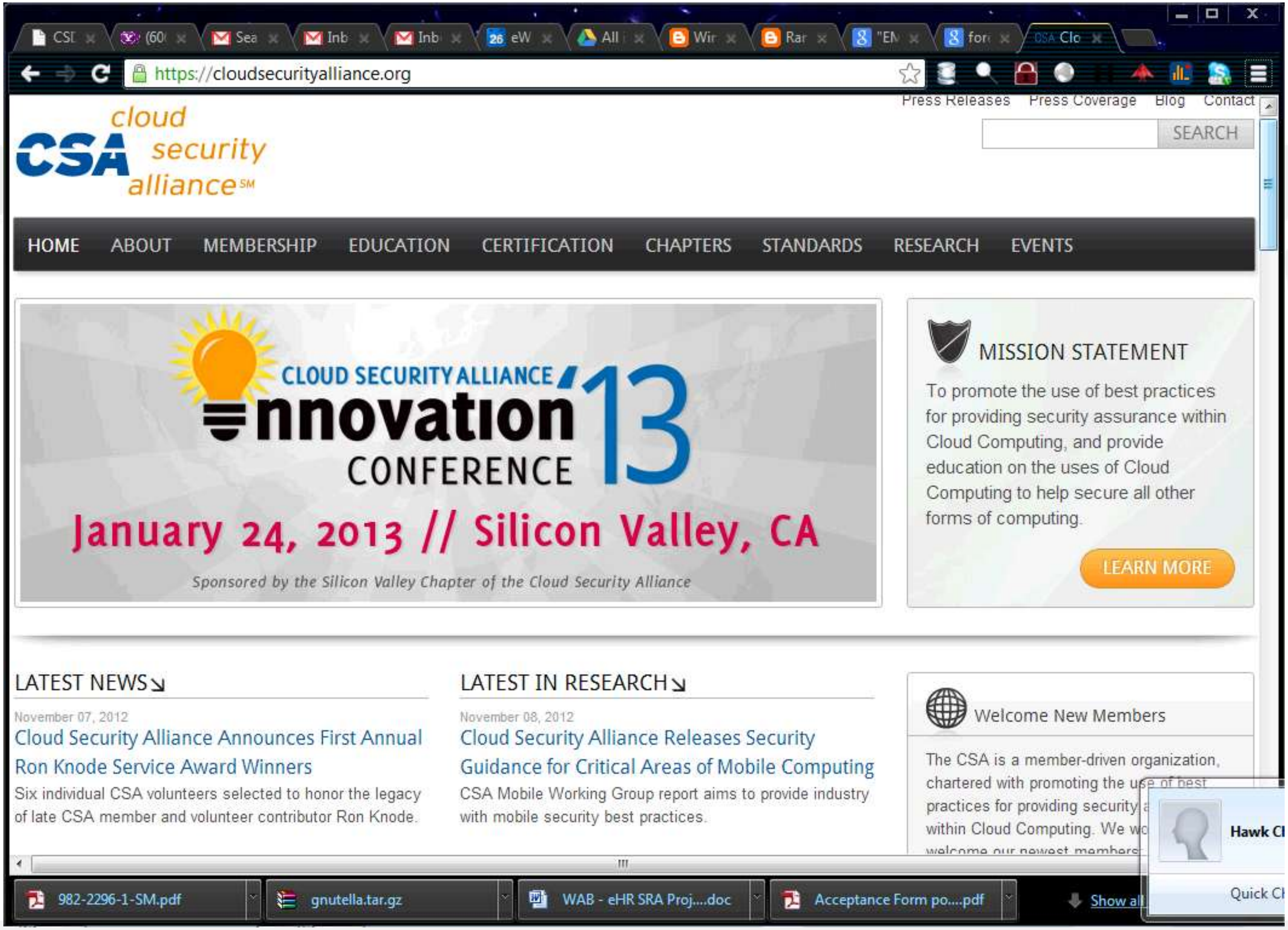
Director of Education

About the Cloud Security Alliance

- Global, not-for-profit organization
- Over 40,000 individual members, around 200 corporate and affiliate members, 64 chapters worldwide
- Building best practices and a trusted cloud ecosystem
- Agile philosophy, rapid development of applied research
  - GRC: Balance compliance with risk management
  - Reference models: build using existing standards
  - Identity: a key foundation of a functioning cloud economy
  - Champion interoperability
  - Enable innovation
  - Advocacy of prudent public policy

"To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing."

Cloud Security Alliance



https://cloudsecurityalliance.org

Press Releases Press Coverage Blog Contact

SEARCH

HOME ABOUT MEMBERSHIP EDUCATION CERTIFICATION CHAPTERS STANDARDS RESEARCH EVENTS

CLOUD SECURITY ALLIANCE Innovation 13 CONFERENCE

January 24, 2013 // Silicon Valley, CA

Sponsored by the Silicon Valley Chapter of the Cloud Security Alliance

MISSION STATEMENT

To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing.

LEARN MORE

LATEST NEWS

November 07, 2012

Cloud Security Alliance Announces First Annual Ron Knode Service Award Winners

Six individual CSA volunteers selected to honor the legacy of late CSA member and volunteer contributor Ron Knode.

LATEST IN RESEARCH

November 08, 2012

Cloud Security Alliance Releases Security Guidance for Critical Areas of Mobile Computing

CSA Mobile Working Group report aims to provide industry with mobile security best practices.

Welcome New Members

The CSA is a member-driven organization, chartered with promoting the use of best practices for providing security within Cloud Computing. We w welcome our newest members

CSA Asia Pacific Expansion

CSA cloud security alliance℠
EDB singapore
iDA
TREND MICRO™
Securing Your Journey to the Cloud

- CSA to set up corporate HQ in Singapore as per joint press release on 20 July 2012
- Founding sponsors of the corporate HQ are IDA, EDB and Trend Micro
- Critical CSA research and projects will be used as an anchor in Singapore:
  - Global CSA Research Centre
  - Global Standards Secretariat
  - Global Centre of Excellence (CoE) for CCSK Training and Education
- Serving as a regional hub and operations magnet for established and emerging growth corporate members
- CSA partners with ASTRI to further APAC Cloud Security Initiatives

CSA Events

CSA
SUMMIT 2012
CLOUD SECURITY ALLIANCE
HONG KONG & MACAU CHAPTERS
17 MAY 2012 // CYBERPORT, HONG KONG

Inauguration of CSA of Hong Kong & Macau Chapter held on May 17, 2012 at Hong Kong’s Cyberport.

http://www.isoc.hk/2012/04/building-trust-in-cloud-computing-summit-2012.html

Top 10 Strategic Technology trends for 2013

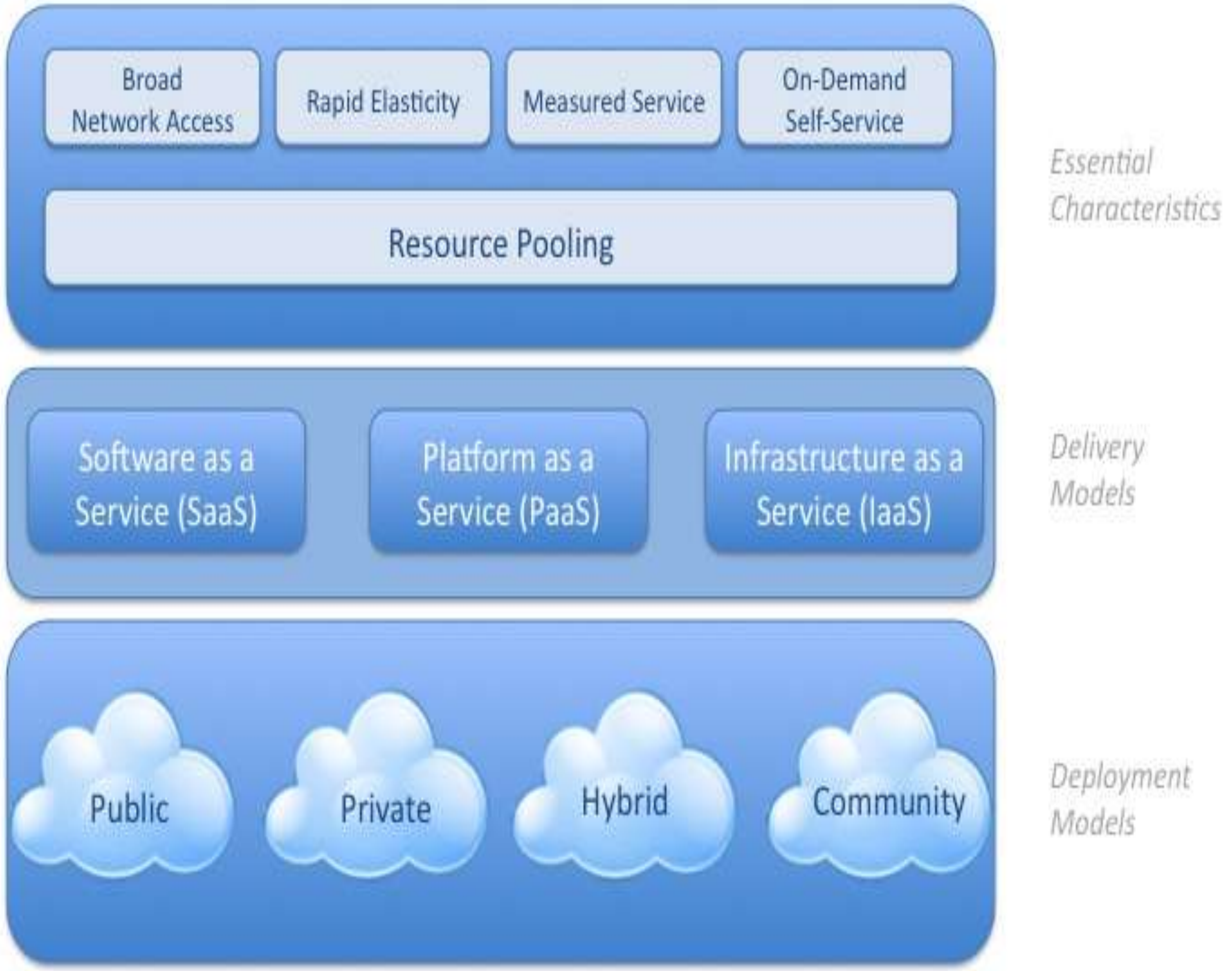
- Mobile Devices Battles
- Mobile Applications & HTML5
- Personal Cloud
- Internet of Things
- Hybrid IT & Cloud Computing
- Strategic Big Data
- Actionable Analytics
- Mainstream In-Memory Computing
- Integrated Ecosystems
- Enterprise App Stores

What is Cloud Computing?

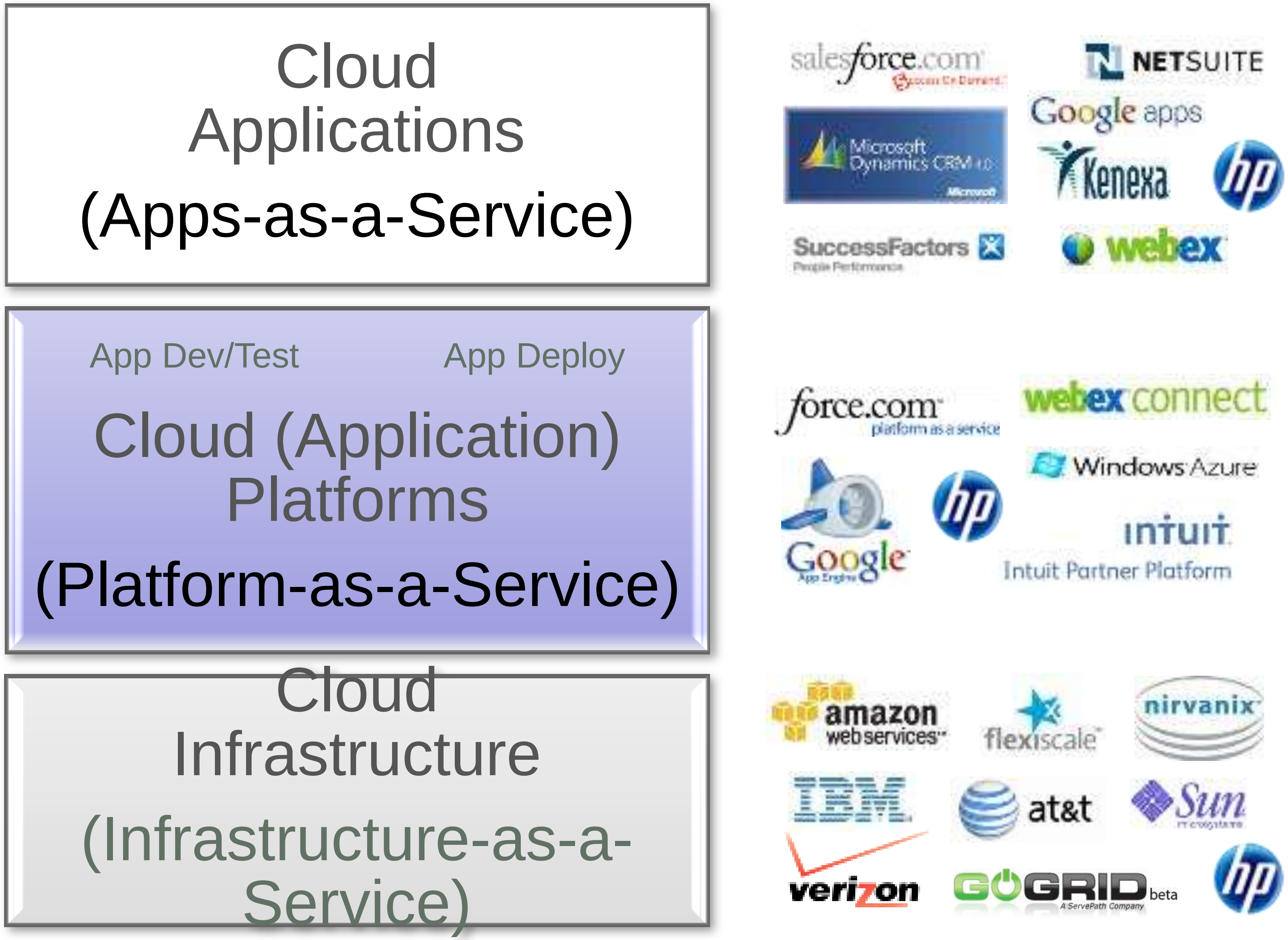
- Compute as a utility: third major era of computing
- Cloud enabled by
  - Moore's Law
  - Hyperconnectivity
  - SOA
  - Provider scale
- Key characteristics
  - Elastic & on-demand
  - Multi-tenancy
  - Metered service

Visual Model Of NIST Working Definition Of Cloud Computing

http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html



Cloud Business?



Cloud Applications

(Apps-as-a-Service)

App Dev/Test

App Deploy

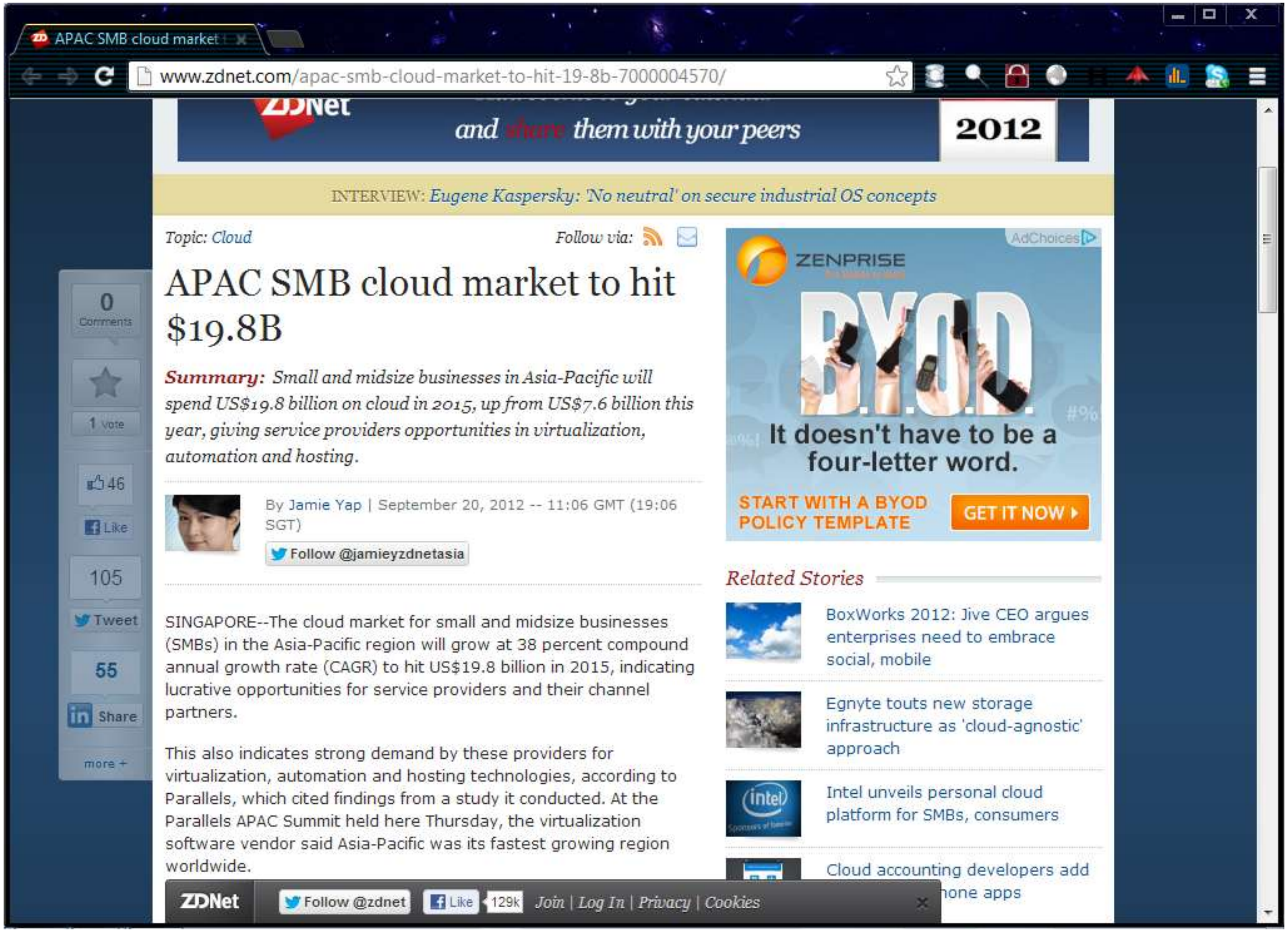
Cloud (Application) Platforms

(Platform-as-a-Service)

Cloud Infrastructure

(Infrastructure-as-a-Service)

APAC SMB cloud market to hit $19.8B in 2015



APAC SMB cloud market
www.zdnet.com/apac-smb-cloud-market-to-hit-19-8b-7000004570/
ZDNet
and share them with your peers
2012

INTERVIEW: *Eugene Kaspersky: 'No neutral' on secure industrial OS concepts*

Topic: Cloud *Follow via:*

APAC SMB cloud market to hit $19.8B

Summary: *Small and midsize businesses in Asia-Pacific will spend US$19.8 billion on cloud in 2015, up from US$7.6 billion this year, giving service providers opportunities in virtualization, automation and hosting.*

By Jamie Yap | September 20, 2012 -- 11:06 GMT (19:06 SGT)

SINGAPORE--The cloud market for small and midsize businesses (SMBs) in the Asia-Pacific region will grow at 38 percent compound annual growth rate (CAGR) to hit US$19.8 billion in 2015, indicating lucrative opportunities for service providers and their channel partners.

This also indicates strong demand by these providers for virtualization, automation and hosting technologies, according to Parallels, which cited findings from a study it conducted. At the Parallels APAC Summit held here Thursday, the virtualization software vendor said Asia-Pacific was its fastest growing region worldwide.

Related Stories

- BoxWorks 2012: Jive CEO argues enterprises need to embrace social, mobile
- Egnyte touts new storage infrastructure as 'cloud-agnostic' approach
- Intel unveils personal cloud platform for SMBs, consumers
- Cloud accounting developers add ...hone apps

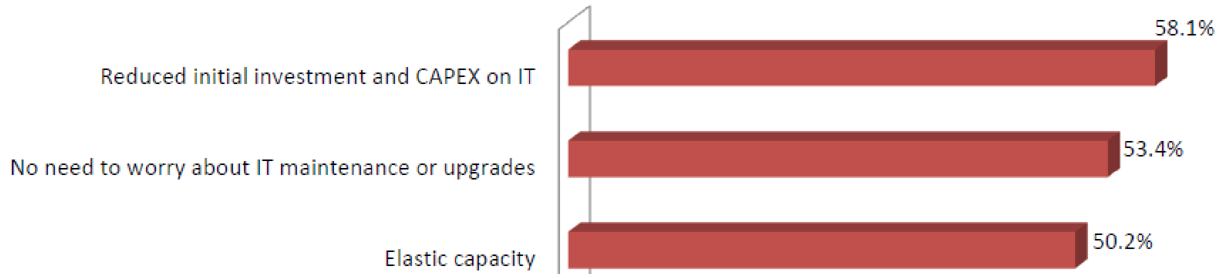
http://www.zdnet.com/apac-smb-cloud-market-to-hit-19-8b-7000004570/

Recent Cloud End User Survey by HKPC

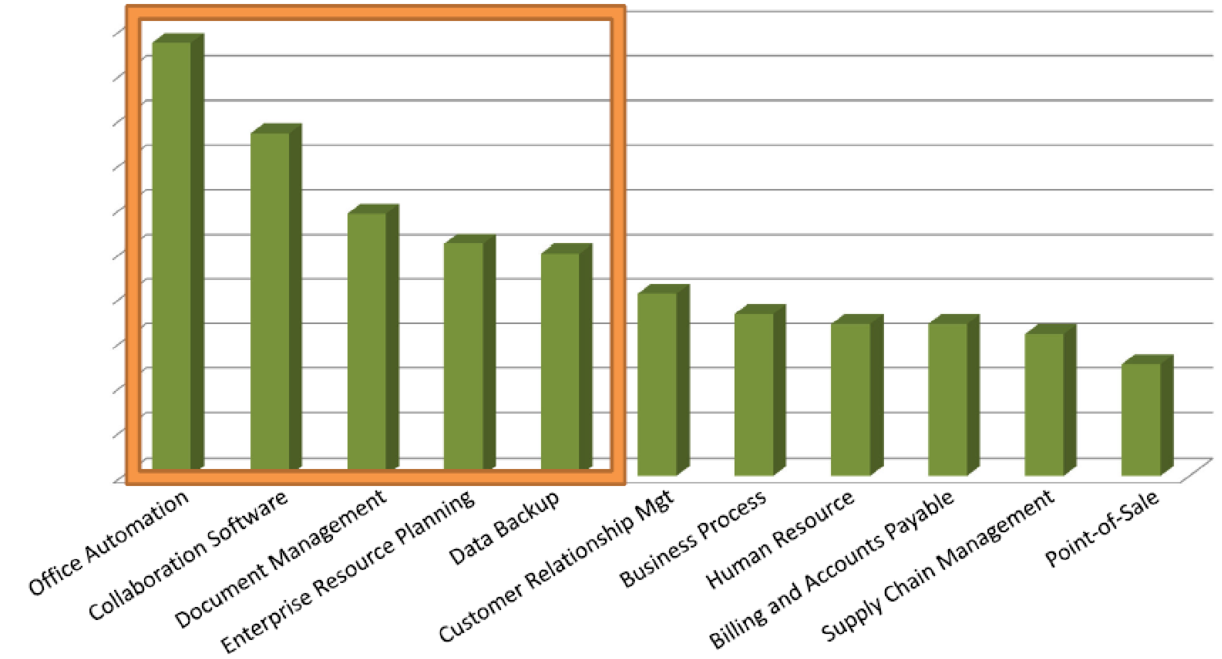
Cloud Adoption

Are You Using Cloud Application?

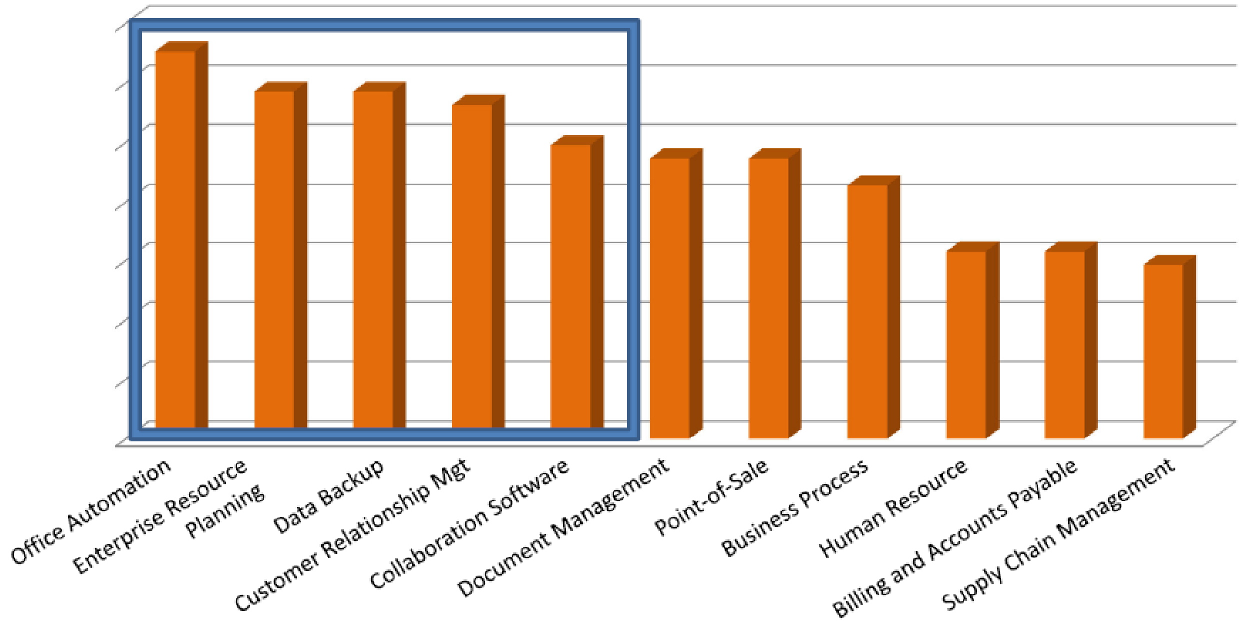
Expected Benefits from Cloud Application



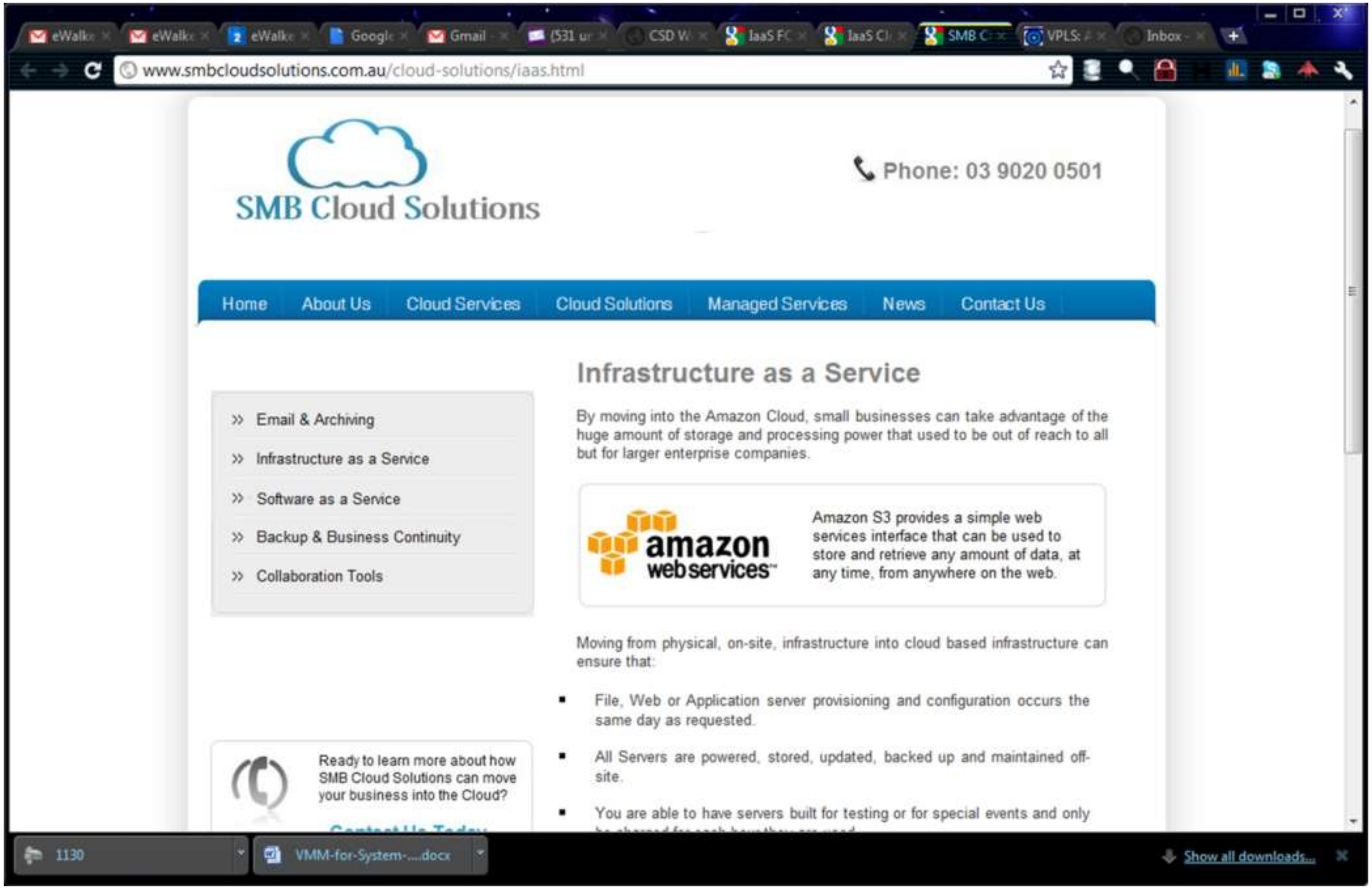
Applications – Currently on Cloud



Applications – To Be on Cloud



SME in the Cloud



SMB Cloud Solutions

☎ Phone: 03 9020 0501

Home | About Us | Cloud Services | Cloud Solutions | Managed Services | News | Contact Us

- » Email & Archiving
- » Infrastructure as a Service
- » Software as a Service
- » Backup & Business Continuity
- » Collaboration Tools

Infrastructure as a Service

By moving into the Amazon Cloud, small businesses can take advantage of the huge amount of storage and processing power that used to be out of reach to all but for larger enterprise companies.

amazon webservices™

Amazon S3 provides a simple web services interface that can be used to store and retrieve any amount of data, at any time, from anywhere on the web.

Moving from physical, on-site, infrastructure into cloud based infrastructure can ensure that:

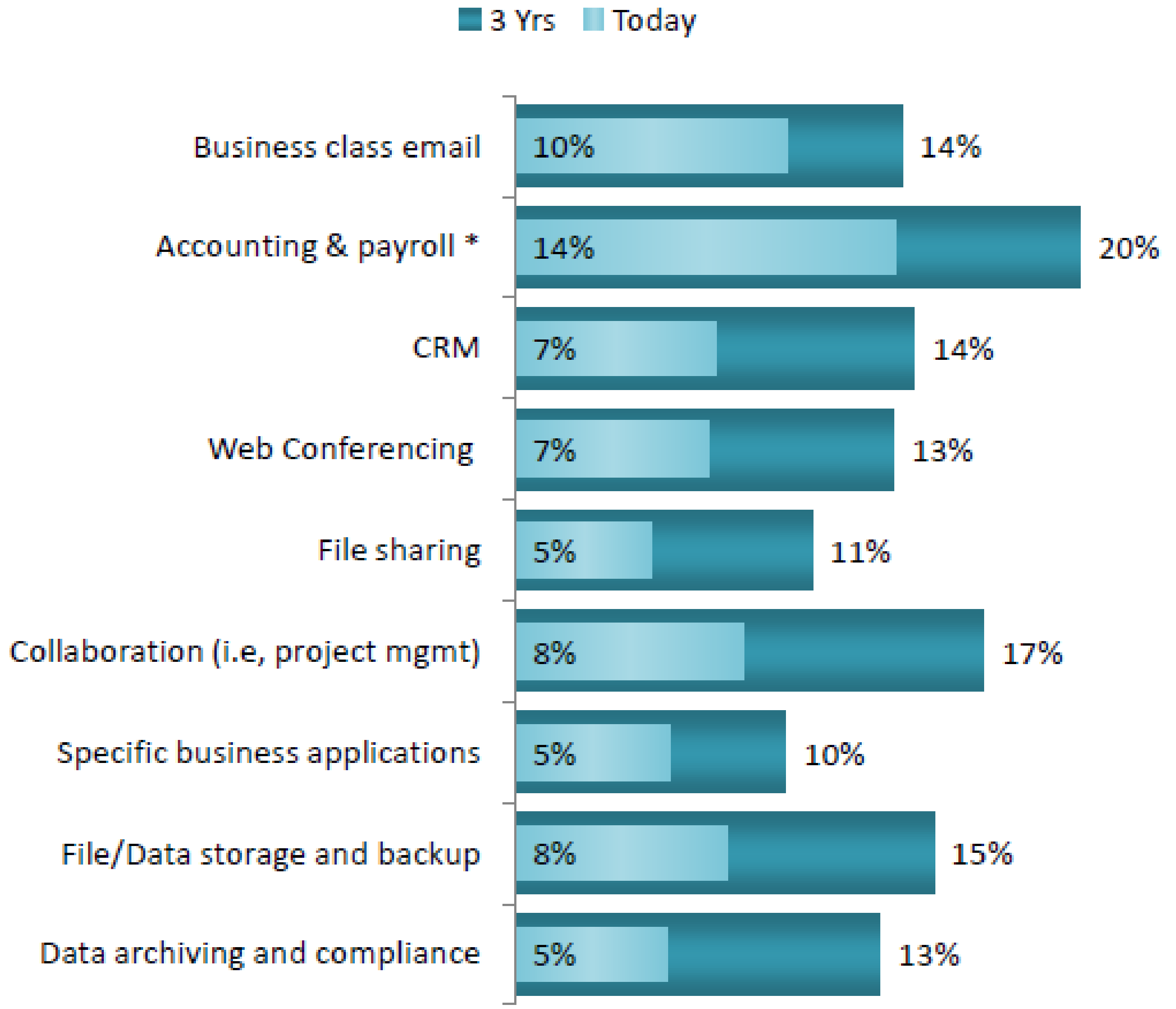
- File, Web or Application server provisioning and configuration occurs the same day as requested.
- All Servers are powered, stored, updated, backed up and maintained off-site.
- You are able to have servers built for testing or for special events and only be charged for each hour they are used.

Ready to learn more about how SMB Cloud Solutions can move your business into the Cloud?

Contact Us Today

cloud security alliance℠

SME Cloud Adoption Study by Microsoft 2011



Workloads Addressed by Paid Cloud Services today and in 3yrs

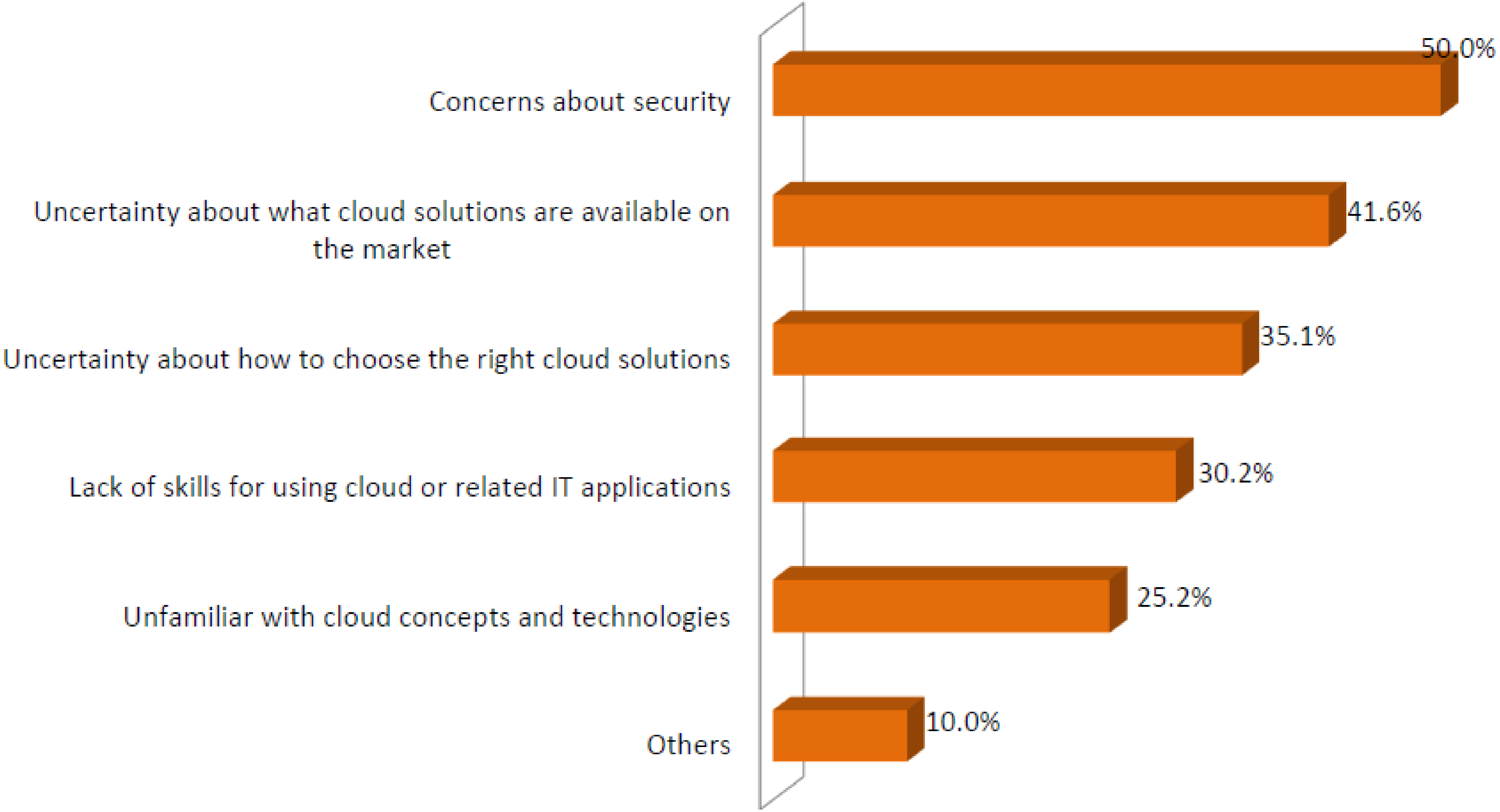
All companies, N=3258

Number of employees
(Today → 3 yrs.)

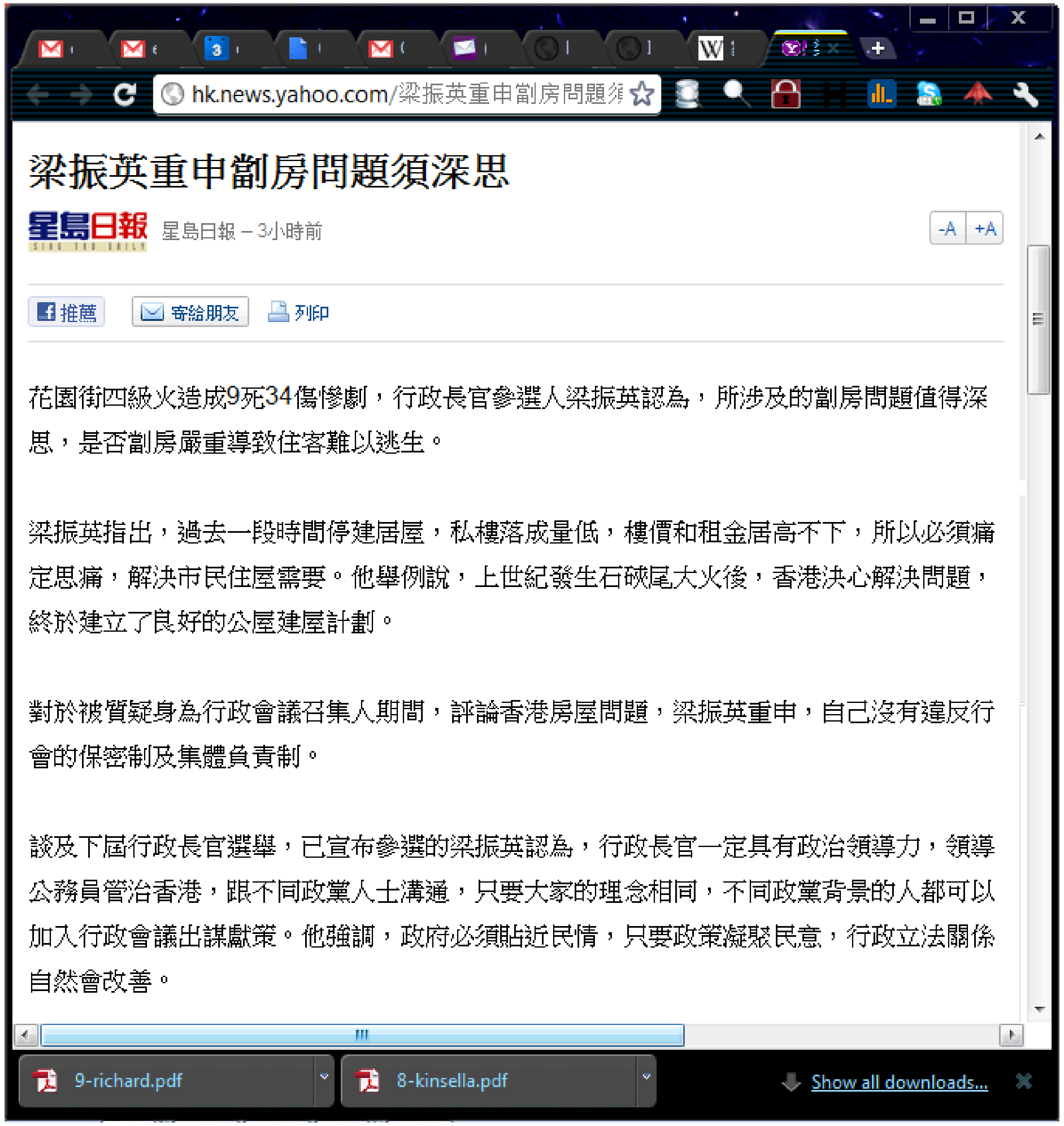
2-10 *N=1180*	11-50 *N=1033*	51-250 *N=1045*
9% → 13%	12% → 16%	15% → 21%
12% → 18%	18% → 25%	24% → 32%
6% → 13%	11% → 17%	15% → 24%
6% → 13%	8% → 15%	11% → 20%
4% → 10%	7% → 13%	11% → 20%
7% → 16%	11% → 18%	18% → 29%
6% → 9%	5% → 11%	7% → 13%
7% → 14%	10% → 18%	12% → 24%
4% → 12%	11% → 17%	11% → 22%

** Reflects companies using hosted service for Payroll*

HKPC Survey – Reasons not using Cloud



Cloud = 劏房??



梁振英重申劏房問題須深思

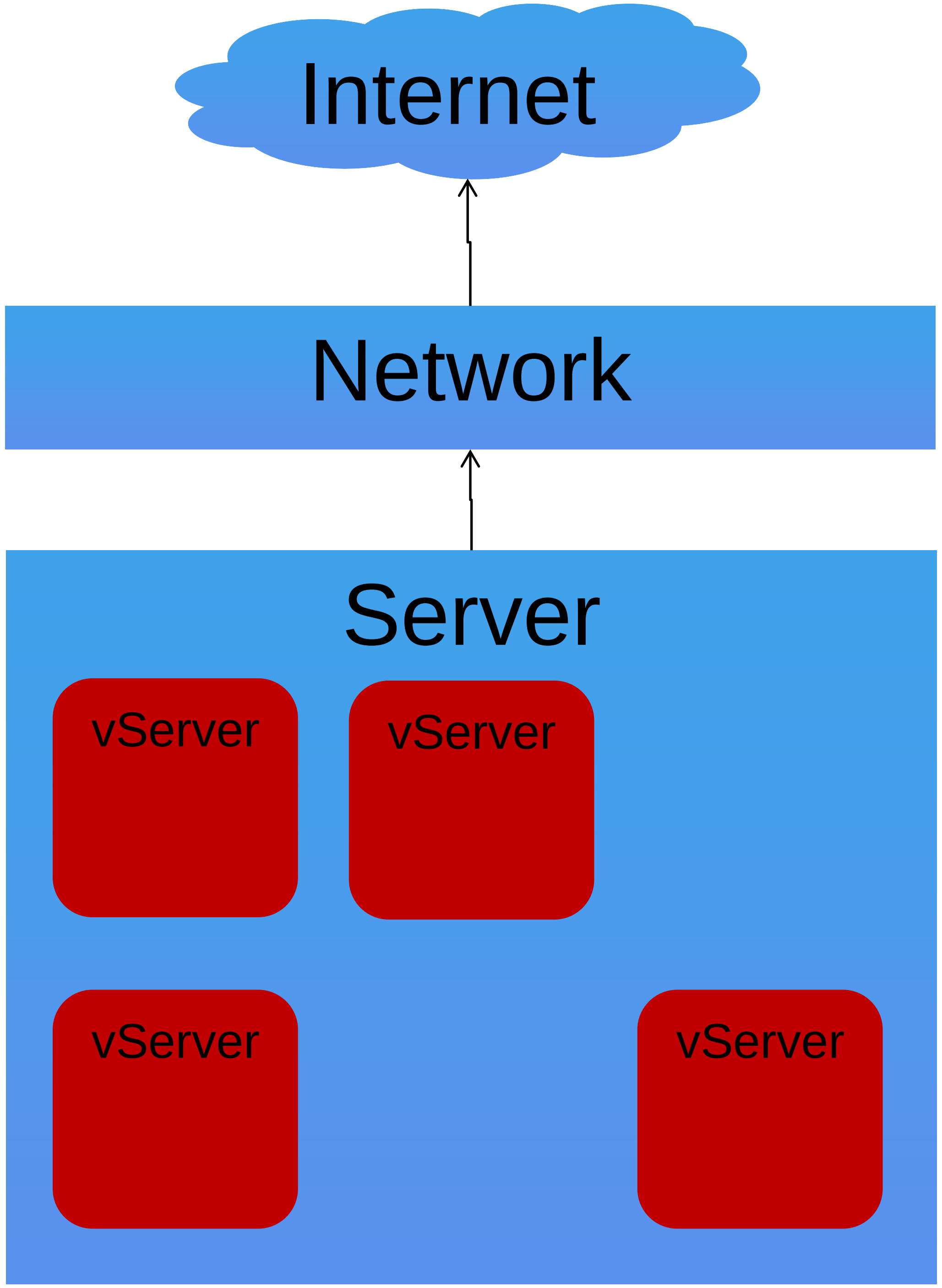
星島日報 – 3小時前

花園街四級火造成9死34傷慘劇，行政長官參選人梁振英認為，所涉及的劏房問題值得深思，是否劏房嚴重導致住客難以逃生。

梁振英指出，過去一段時間停建居屋，私樓落成量低，樓價和租金居高不下，所以必須痛定思痛，解決市民住屋需要。他舉例說，上世紀發生石硤尾大火後，香港決心解決問題，終於建立了良好的公屋建屋計劃。

對於被質疑身為行政會議召集人期間，評論香港房屋問題，梁振英重申，自己沒有違反行會的保密制及集體負責制。

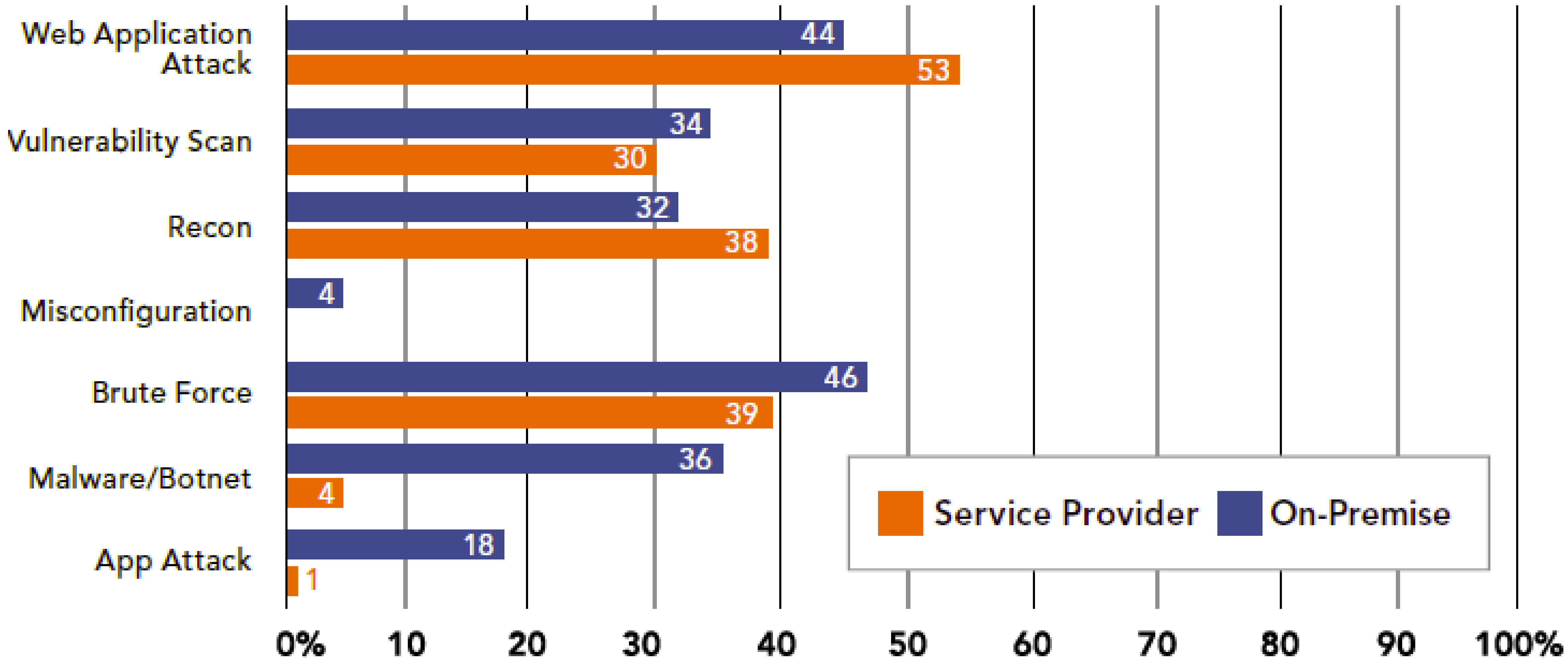
談及下屆行政長官選舉，已宣布參選的梁振英認為，行政長官一定具有政治領導力，領導公務員管治香港，跟不同政黨人士溝通，只要大家的理念相同，不同政黨背景的人都可以加入行政會議出謀獻策。他強調，政府必須貼近民情，只要政策凝聚民意，行政立法關係自然會改善。



Latest Attack report on Cloud Security

FIG. C

INCIDENT OCCURRENCE:
TOP THREE INCIDENT CLASSES

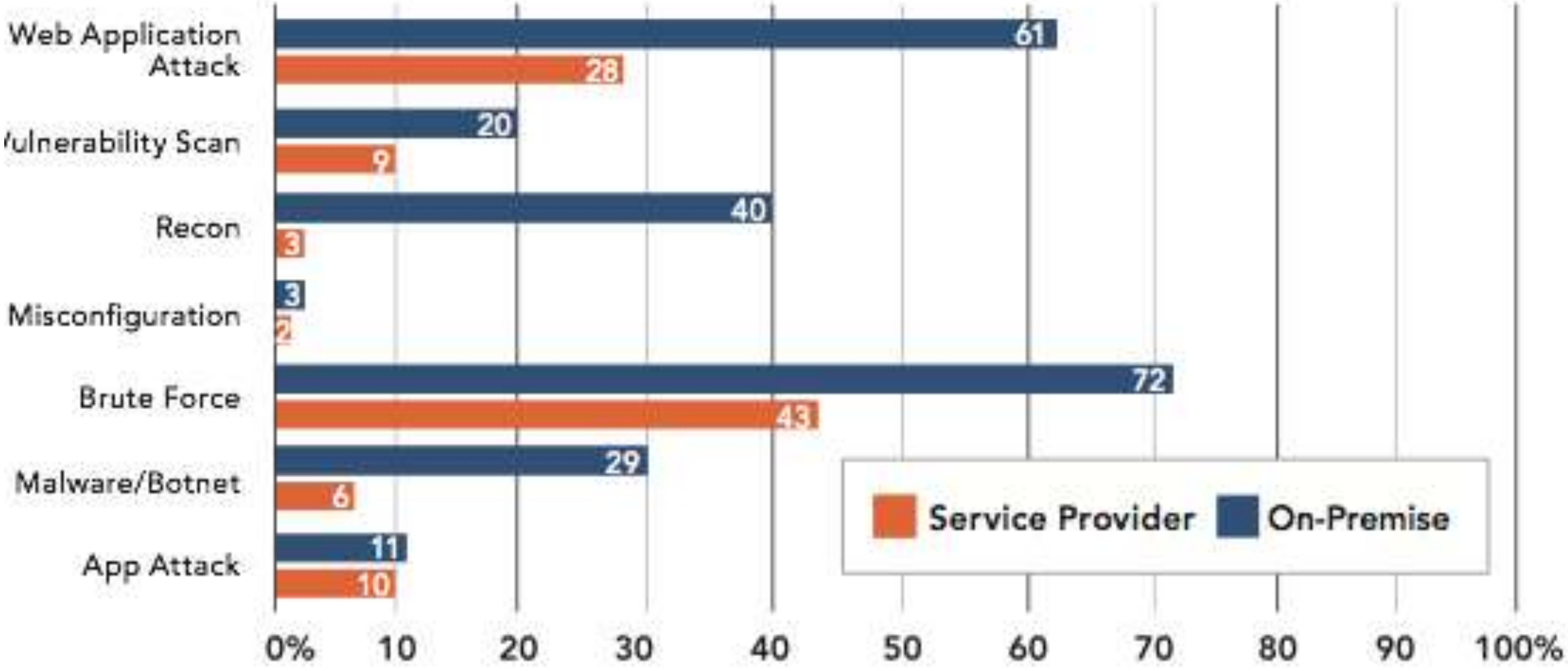


Alert Logic State of Cloud Security Report Fall 2012

Latest Attack report on Cloud Security

FIG. D

INCIDENT FREQUENCY:
NUMBER OF INCIDENTS PER IMPACTED CUSTOMER

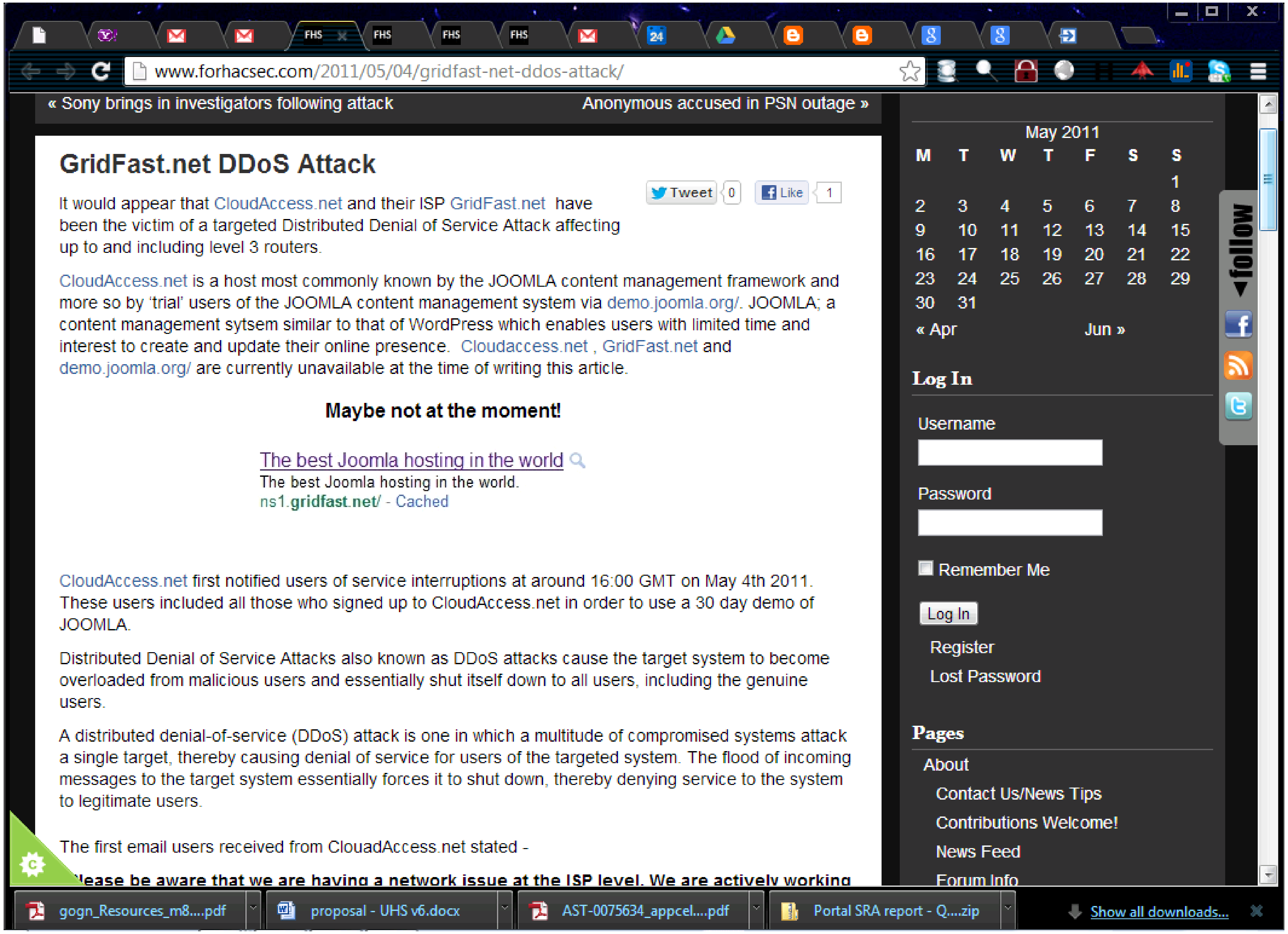


Alert Logic State of Cloud Security Report Fall 2012

Latest Attack report on Cloud Security

- Other key points:
  - IT Services companies that have a public presence experienced a large number of Web application attacks
  - E-commerce and SaaS environments are frequent targets of scanning
  - Malware is seen more frequently in Financial Services
  - A significant number of Media companies are being targeted by hacktivists

CloudAccess.net attacked by DDoS



www.forhacsec.com/2011/05/04/gridfast-net-ddos-attack/
« Sony brings in investigators following attack
Anonymous accused in PSN outage »
Tweet 0
Like 1
follow
gogn_Resources_m8....pdf
proposal - UHS v6.docx
AST-0075634_appcel....pdf
Portal SRA report - Q....zip
Show all downloads...

GridFast.net DDoS Attack

It would appear that CloudAccess.net and their ISP GridFast.net have been the victim of a targeted Distributed Denial of Service Attack affecting up to and including level 3 routers.

CloudAccess.net is a host most commonly known by the JOOMLA content management framework and more so by 'trial' users of the JOOMLA content management system via demo.joomla.org/. JOOMLA; a content management sytsem similar to that of WordPress which enables users with limited time and interest to create and update their online presence. Cloudaccess.net , GridFast.net and demo.joomla.org/ are currently unavailable at the time of writing this article.

Maybe not at the moment!

The best Joomla hosting in the world
The best Joomla hosting in the world.
ns1.gridfast.net/ - Cached

CloudAccess.net first notified users of service interruptions at around 16:00 GMT on May 4th 2011. These users included all those who signed up to CloudAccess.net in order to use a 30 day demo of JOOMLA.

Distributed Denial of Service Attacks also known as DDoS attacks cause the target system to become overloaded from malicious users and essentially shut itself down to all users, including the genuine users.

A distributed denial-of-service (DDoS) attack is one in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The flood of incoming messages to the target system essentially forces it to shut down, thereby denying service to the system to legitimate users.

The first email users received from ClouadAccess.net stated -

Please be aware that we are having a network issue at the ISP level. We are actively working

May 2011						
M	T	W	T	F	S	S
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

« Apr Jun »

Log In

Username

Password

□ Remember Me

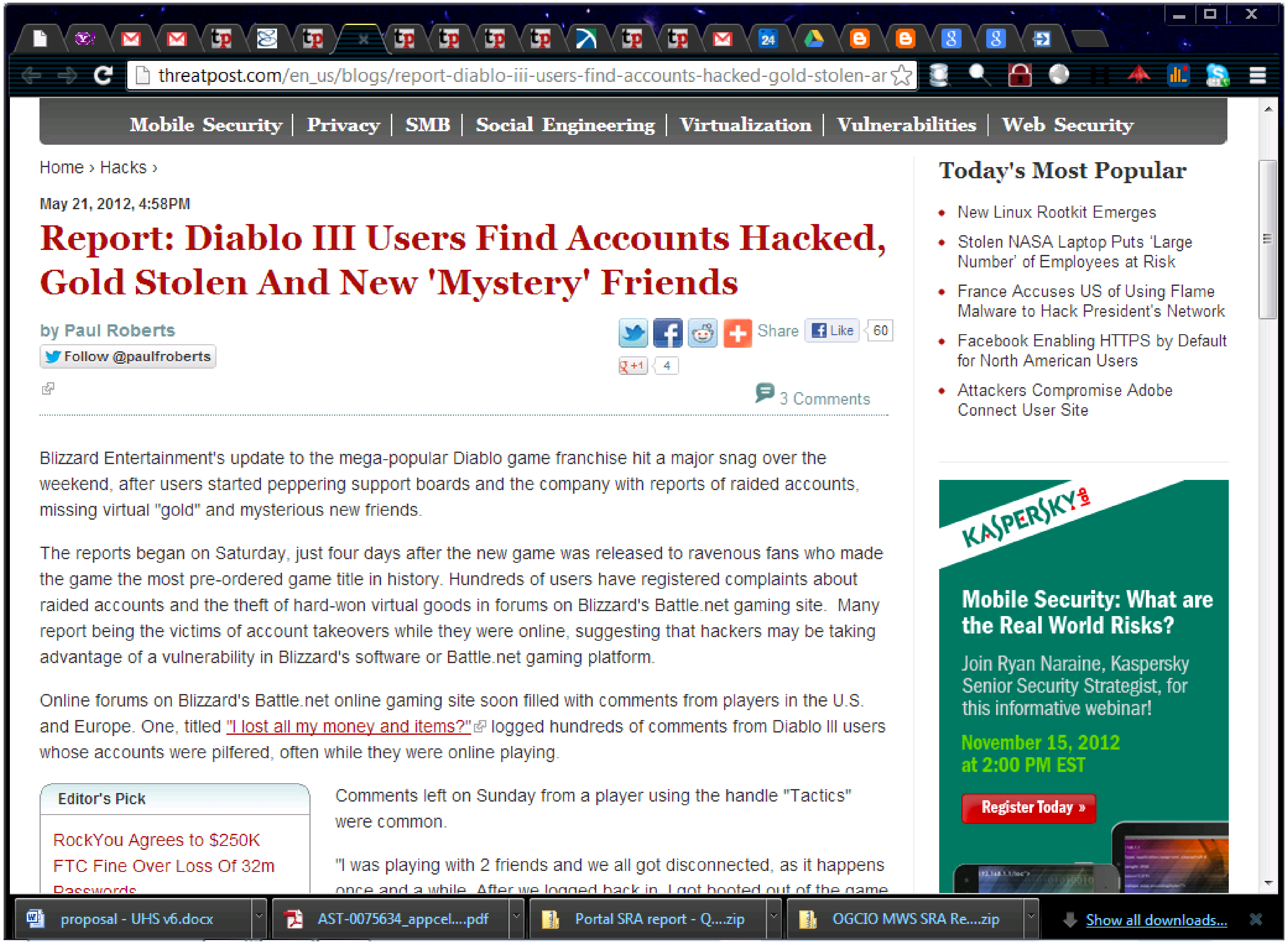
Log In

Register
Lost Password

Pages

About
Contact Us/News Tips
Contributions Welcome!
News Feed
Forum Info

Diablo III Users account hacked



threatpost.com/en_us/blogs/report-diablo-iii-users-find-accounts-hacked-gold-stolen-ar
Mobile Security | Privacy | SMB | Social Engineering | Virtualization | Vulnerabilities | Web Security

Home › Hacks ›

May 21, 2012, 4:58PM

Report: Diablo III Users Find Accounts Hacked, Gold Stolen And New 'Mystery' Friends

by Paul Roberts

Follow @paulfroberts
Share
Like
60
+1
4
3 Comments

Blizzard Entertainment's update to the mega-popular Diablo game franchise hit a major snag over the weekend, after users started peppering support boards and the company with reports of raided accounts, missing virtual "gold" and mysterious new friends.

The reports began on Saturday, just four days after the new game was released to ravenous fans who made the game the most pre-ordered game title in history. Hundreds of users have registered complaints about raided accounts and the theft of hard-won virtual goods in forums on Blizzard's Battle.net gaming site. Many report being the victims of account takeovers while they were online, suggesting that hackers may be taking advantage of a vulnerability in Blizzard's software or Battle.net gaming platform.

Online forums on Blizzard's Battle.net online gaming site soon filled with comments from players in the U.S. and Europe. One, titled "I lost all my money and items?" logged hundreds of comments from Diablo III users whose accounts were pilfered, often while they were online playing.

Editor's Pick

RockYou Agrees to $250K FTC Fine Over Loss Of 32m Passwords

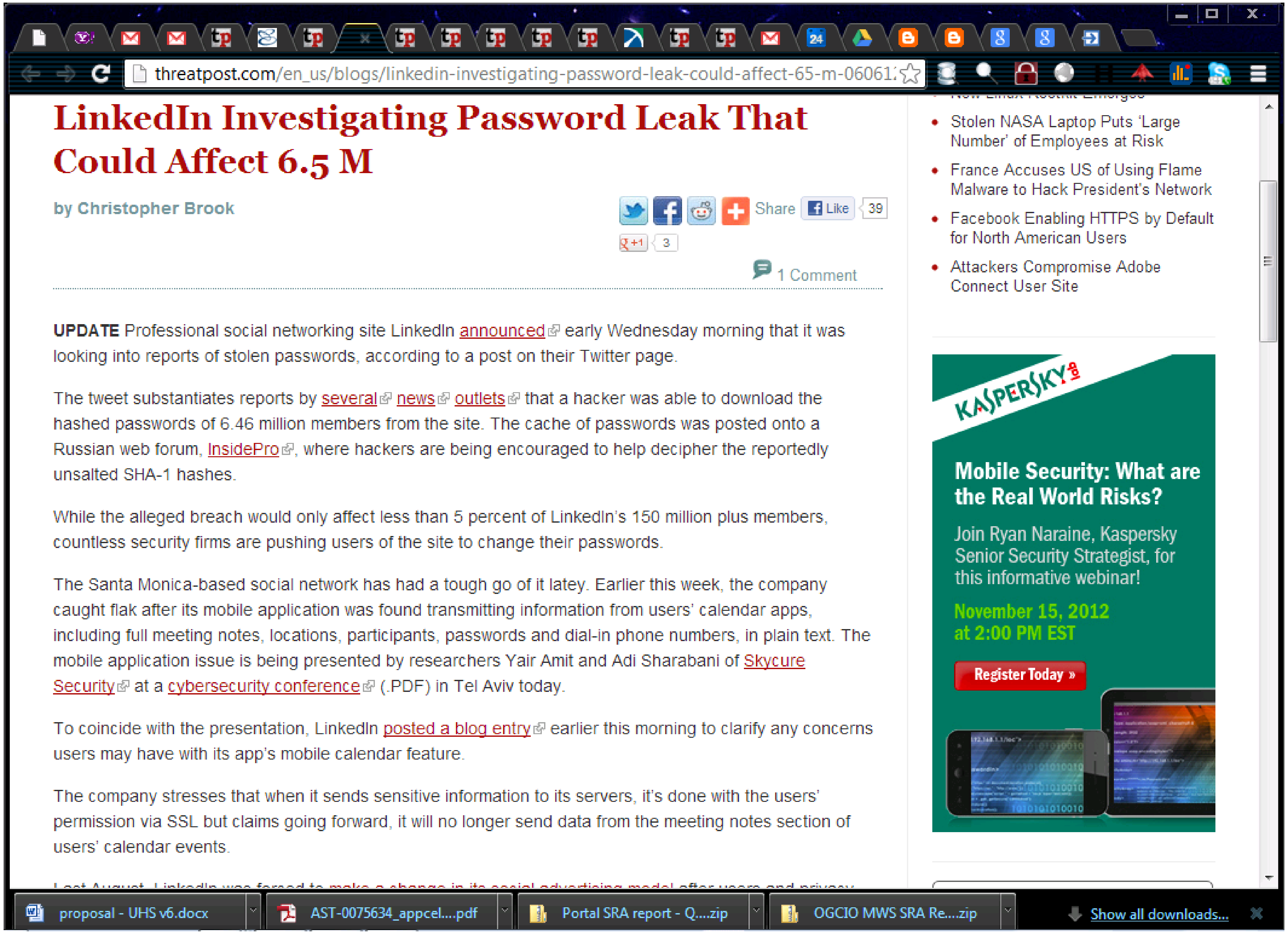
Comments left on Sunday from a player using the handle "Tactics" were common.

"I was playing with 2 friends and we all got disconnected, as it happens once and a while. After we logged back in, I got booted out of the game

Today's Most Popular

- New Linux Rootkit Emerges
- Stolen NASA Laptop Puts 'Large Number' of Employees at Risk
- France Accuses US of Using Flame Malware to Hack President's Network
- Facebook Enabling HTTPS by Default for North American Users
- Attackers Compromise Adobe Connect User Site

LinkedIn 6.5 million password hashed stolen



threatpost.com/en_us/blogs/linkedin-investigating-password-leak-could-affect-65-m-06061

LinkedIn Investigating Password Leak That Could Affect 6.5 M

by Christopher Brook

Share
Like
39
+1
3
1 Comment

UPDATE Professional social networking site LinkedIn announced early Wednesday morning that it was looking into reports of stolen passwords, according to a post on their Twitter page.

The tweet substantiates reports by several news outlets that a hacker was able to download the hashed passwords of 6.46 million members from the site. The cache of passwords was posted onto a Russian web forum, InsidePro, where hackers are being encouraged to help decipher the reportedly unsalted SHA-1 hashes.

While the alleged breach would only affect less than 5 percent of LinkedIn's 150 million plus members, countless security firms are pushing users of the site to change their passwords.

The Santa Monica-based social network has had a tough go of it latey. Earlier this week, the company caught flak after its mobile application was found transmitting information from users' calendar apps, including full meeting notes, locations, participants, passwords and dial-in phone numbers, in plain text. The mobile application issue is being presented by researchers Yair Amit and Adi Sharabani of Skycure Security at a cybersecurity conference (.PDF) in Tel Aviv today.

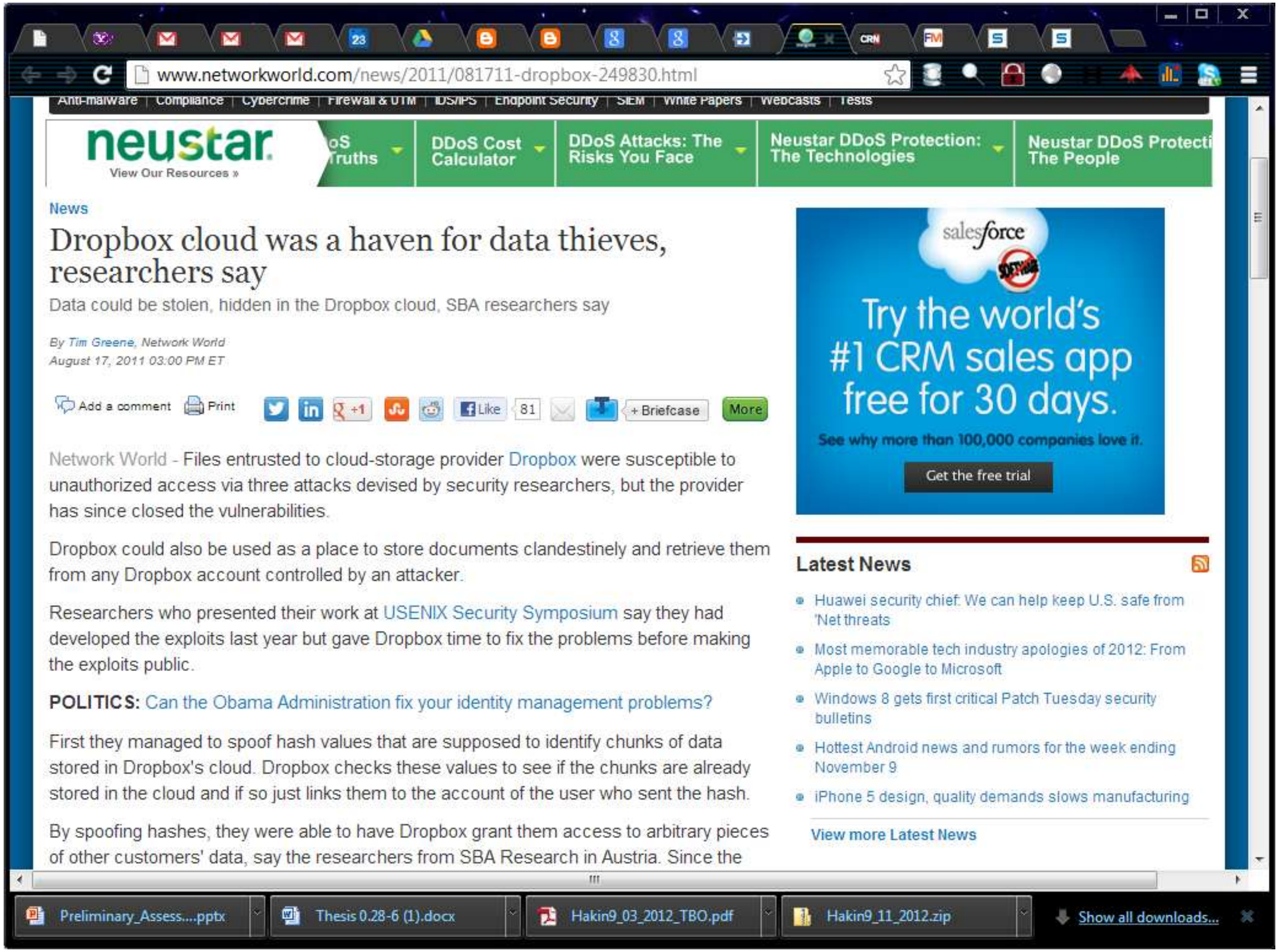
To coincide with the presentation, LinkedIn posted a blog entry earlier this morning to clarify any concerns users may have with its app's mobile calendar feature.

The company stresses that when it sends sensitive information to its servers, it's done with the users' permission via SSL but claims going forward, it will no longer send data from the meeting notes section of users' calendar events.

Last August, LinkedIn was forced to make a change in its social advertising model after users and privacy

- New Linux Rootkit Emerges
- Stolen NASA Laptop Puts 'Large Number' of Employees at Risk
- France Accuses US of Using Flame Malware to Hack President's Network
- Facebook Enabling HTTPS by Default for North American Users
- Attackers Compromise Adobe Connect User Site

Data Security in Cloud Starts from users


www.networkworld.com/news/2011/081711-dropbox-249830.html
Anti-malware | Compliance | Cybercrime | Firewall & UTM | IDS/IPS | Endpoint Security | SIEM | White Papers | Webcasts | Tests
neustar
View Our Resources »
oS Truths
DDoS Cost Calculator
DDoS Attacks: The Risks You Face
Neustar DDoS Protection: The Technologies
Neustar DDoS Protecti The People
Add a comment
Print
+1
Like
81
+ Briefcase
More
Preliminary_Assess....pptx
Thesis 0.28-6 (1).docx
Hakin9_03_2012_TBO.pdf
Hakin9_11_2012.zip
Show all downloads...

News

Dropbox cloud was a haven for data thieves, researchers say

Data could be stolen, hidden in the Dropbox cloud, SBA researchers say

By Tim Greene, Network World
August 17, 2011 03:00 PM ET

Network World - Files entrusted to cloud-storage provider Dropbox were susceptible to unauthorized access via three attacks devised by security researchers, but the provider has since closed the vulnerabilities.

Dropbox could also be used as a place to store documents clandestinely and retrieve them from any Dropbox account controlled by an attacker.

Researchers who presented their work at USENIX Security Symposium say they had developed the exploits last year but gave Dropbox time to fix the problems before making the exploits public.

POLITICS: Can the Obama Administration fix your identity management problems?

First they managed to spoof hash values that are supposed to identify chunks of data stored in Dropbox's cloud. Dropbox checks these values to see if the chunks are already stored in the cloud and if so just links them to the account of the user who sent the hash.

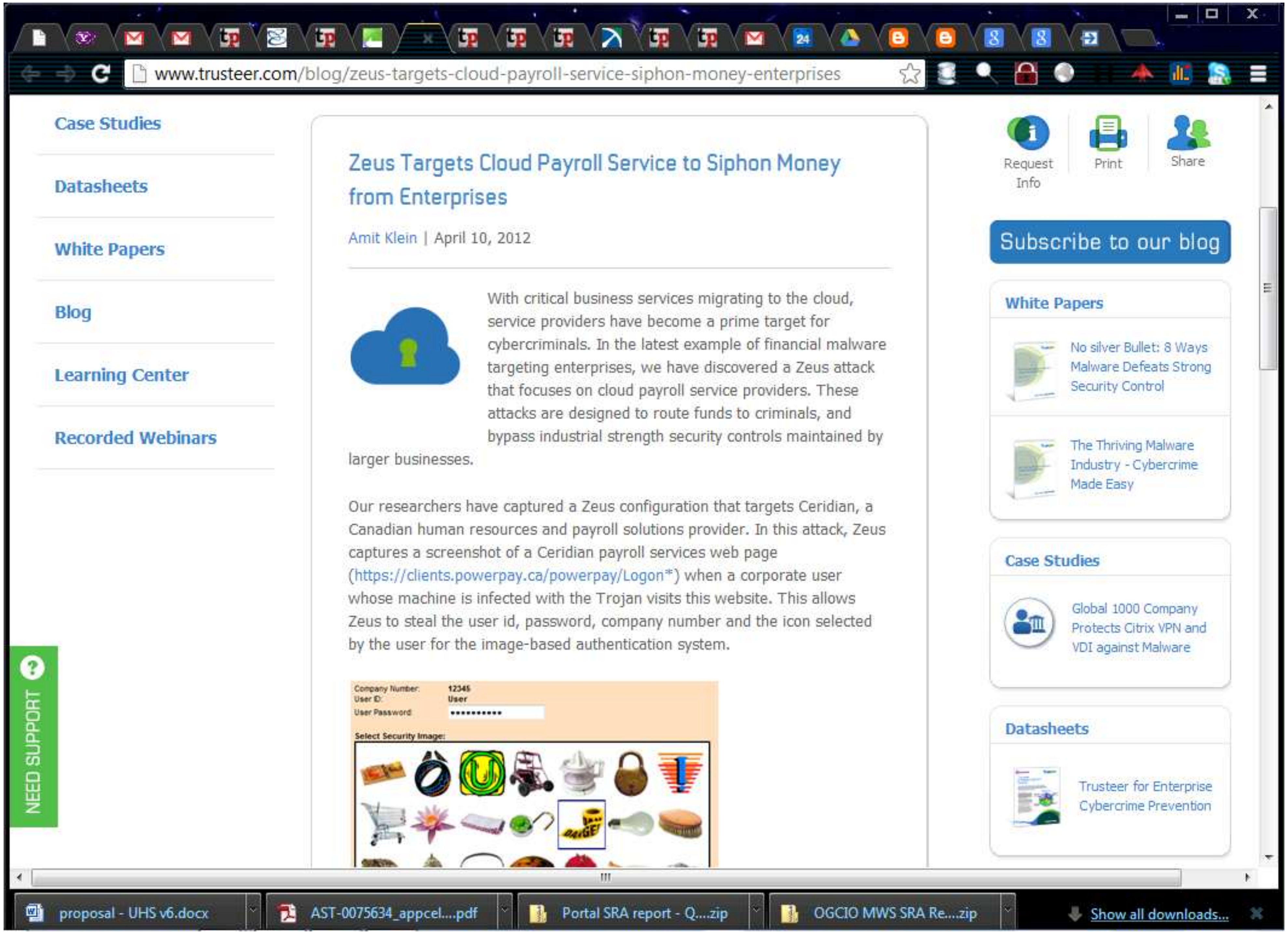
By spoofing hashes, they were able to have Dropbox grant them access to arbitrary pieces of other customers' data, say the researchers from SBA Research in Austria. Since the

Latest News

- Huawei security chief: We can help keep U.S. safe from 'Net threats
- Most memorable tech industry apologies of 2012: From Apple to Google to Microsoft
- Windows 8 gets first critical Patch Tuesday security bulletins
- Hottest Android news and rumors for the week ending November 9
- iPhone 5 design, quality demands slows manufacturing

View more Latest News

Zeus Targets Cloud Payroll Services



Zeus Targets Cloud Payroll Service to Siphon Money from Enterprises

Amit Klein | April 10, 2012

With critical business services migrating to the cloud, service providers have become a prime target for cybercriminals. In the latest example of financial malware targeting enterprises, we have discovered a Zeus attack that focuses on cloud payroll service providers. These attacks are designed to route funds to criminals, and bypass industrial strength security controls maintained by larger businesses.

Our researchers have captured a Zeus configuration that targets Ceridian, a Canadian human resources and payroll solutions provider. In this attack, Zeus captures a screenshot of a Ceridian payroll services web page (https://clients.powerpay.ca/powerpay/Logon*) when a corporate user whose machine is infected with the Trojan visits this website. This allows Zeus to steal the user id, password, company number and the icon selected by the user for the image-based authentication system.

Company Number: 12345
User ID: User
User Password: •••••••••••

Select Security Image:

White Papers

No silver Bullet: 8 Ways Malware Defeats Strong Security Control

The Thriving Malware Industry - Cybercrime Made Easy

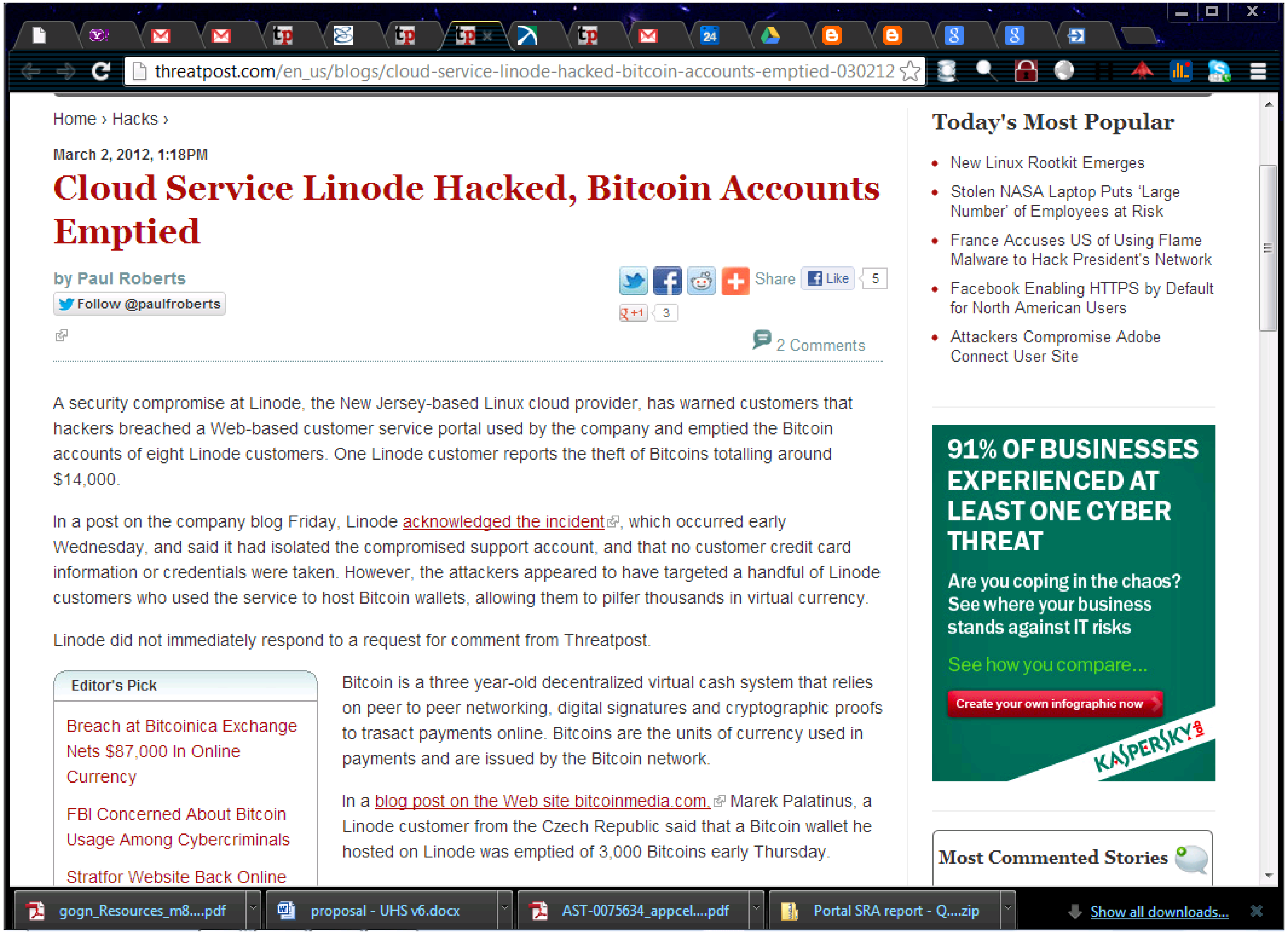
Case Studies

Global 1000 Company Protects Citrix VPN and VDI against Malware

Datasheets

Trusteer for Enterprise Cybercrime Prevention

Cloud Service Linode Hacked, Bitcoin Accounts Emptied



threatpost.com/en_us/blogs/cloud-service-linode-hacked-bitcoin-accounts-emptied-030212

Home › Hacks ›

March 2, 2012, 1:18PM

Cloud Service Linode Hacked, Bitcoin Accounts Emptied

by Paul Roberts
Follow @paulfroberts

2 Comments

A security compromise at Linode, the New Jersey-based Linux cloud provider, has warned customers that hackers breached a Web-based customer service portal used by the company and emptied the Bitcoin accounts of eight Linode customers. One Linode customer reports the theft of Bitcoins totalling around $14,000.

In a post on the company blog Friday, Linode acknowledged the incident, which occurred early Wednesday, and said it had isolated the compromised support account, and that no customer credit card information or credentials were taken. However, the attackers appeared to have targeted a handful of Linode customers who used the service to host Bitcoin wallets, allowing them to pilfer thousands in virtual currency.

Linode did not immediately respond to a request for comment from Threatpost.

Editor's Pick

- Breach at Bitcoinica Exchange Nets $87,000 In Online Currency
- FBI Concerned About Bitcoin Usage Among Cybercriminals
- Stratfor Website Back Online

Bitcoin is a three year-old decentralized virtual cash system that relies on peer to peer networking, digital signatures and cryptographic proofs to trasact payments online. Bitcoins are the units of currency used in payments and are issued by the Bitcoin network.

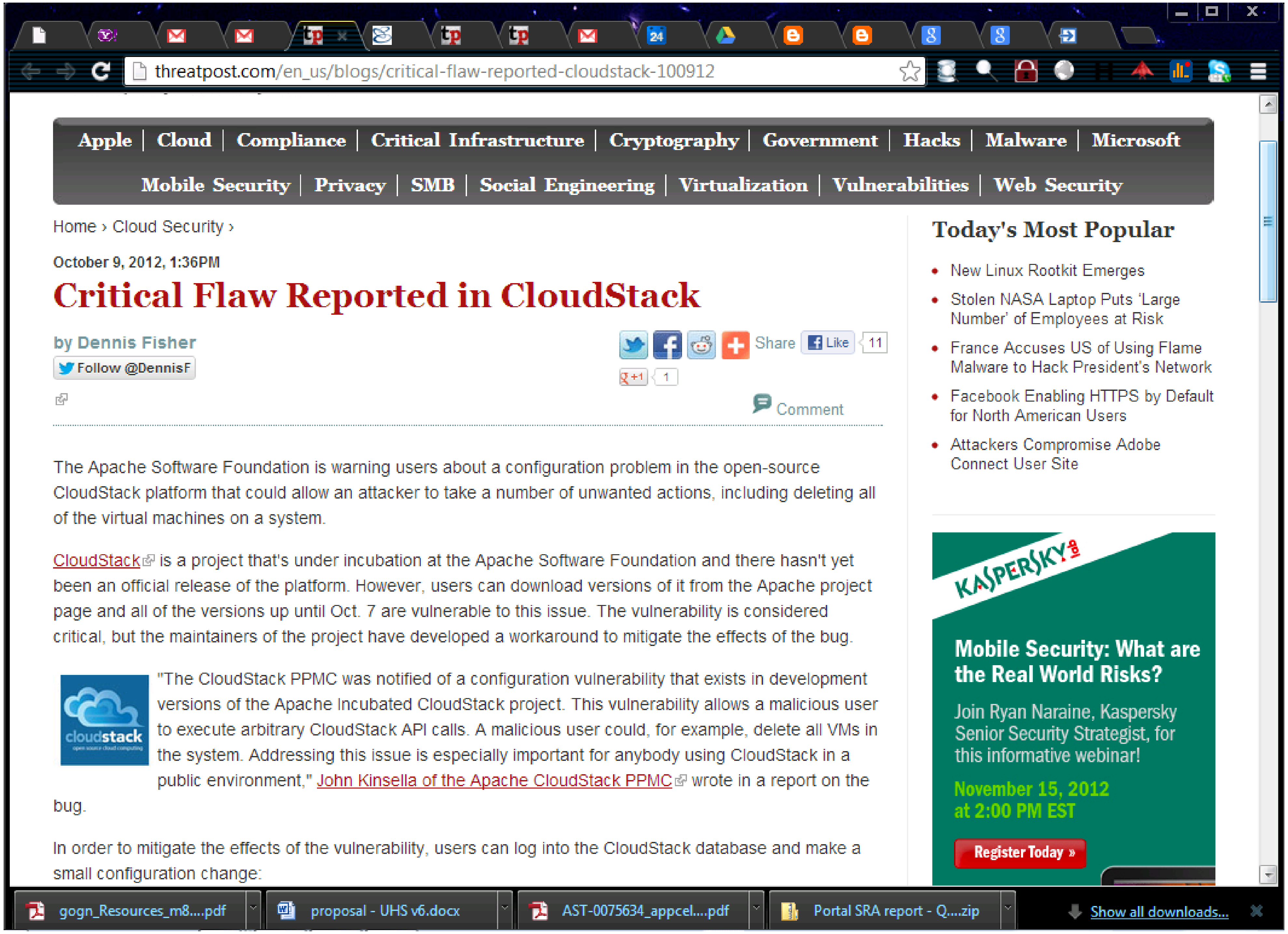
In a blog post on the Web site bitcoinmedia.com, Marek Palatinus, a Linode customer from the Czech Republic said that a Bitcoin wallet he hosted on Linode was emptied of 3,000 Bitcoins early Thursday.

Today's Most Popular

- New Linux Rootkit Emerges
- Stolen NASA Laptop Puts 'Large Number' of Employees at Risk
- France Accuses US of Using Flame Malware to Hack President's Network
- Facebook Enabling HTTPS by Default for North American Users
- Attackers Compromise Adobe Connect User Site

Most Commented Stories

CloudStack Critical Vulnerability


threatpost.com/en_us/blogs/critical-flaw-reported-cloudstack-100912
Apple | Cloud | Compliance | Critical Infrastructure | Cryptography | Government | Hacks | Malware | Microsoft
Mobile Security | Privacy | SMB | Social Engineering | Virtualization | Vulnerabilities | Web Security
Follow @DennisF
Share
Like
11
+1
1
Comment
cloudstack
gogn_Resources_m8....pdf
proposal - UHS v6.docx
AST-0075634_appcel....pdf
Portal SRA report - Q....zip
Show all downloads...

Home › Cloud Security ›

October 9, 2012, 1:36PM

Critical Flaw Reported in CloudStack

by Dennis Fisher

The Apache Software Foundation is warning users about a configuration problem in the open-source CloudStack platform that could allow an attacker to take a number of unwanted actions, including deleting all of the virtual machines on a system.

CloudStack is a project that's under incubation at the Apache Software Foundation and there hasn't yet been an official release of the platform. However, users can download versions of it from the Apache project page and all of the versions up until Oct. 7 are vulnerable to this issue. The vulnerability is considered critical, but the maintainers of the project have developed a workaround to mitigate the effects of the bug.

"The CloudStack PPMC was notified of a configuration vulnerability that exists in development versions of the Apache Incubated CloudStack project. This vulnerability allows a malicious user to execute arbitrary CloudStack API calls. A malicious user could, for example, delete all VMs in the system. Addressing this issue is especially important for anybody using CloudStack in a public environment," John Kinsella of the Apache CloudStack PPMC wrote in a report on the bug.

In order to mitigate the effects of the vulnerability, users can log into the CloudStack database and make a small configuration change:

Today's Most Popular

- New Linux Rootkit Emerges
- Stolen NASA Laptop Puts 'Large Number' of Employees at Risk
- France Accuses US of Using Flame Malware to Hack President's Network
- Facebook Enabling HTTPS by Default for North American Users
- Attackers Compromise Adobe Connect User Site

Self-assessment questions

- Evaluate what is critical to business?
- What's the purpose of cloud service?
- How to prepare for data protection?
- How to continuous monitor the incident?
- How to preserve evidence if any incident happened?

Don’t Overlook the A-Z of Cloud Security

1. Selection of Cloud Service Provider

2. Contractual and Commercial Terms

3. Access Control

4. Data Protection

5. Cloud Administration

6. Service Continuity

1. Selection of Cloud Service Provider

a) Understand risks and determine acceptance levels

b) Select those who can explain their security features, preferred to have attained security certification

c) Select those with service level agreements commensurable with the importance of the business function

d) Select those who can provide secure channels for transmitting and storing sensitive data

e) Select those with good reputation with no major reported security incidents

2. Contractual and Commercial Terms

f) Understand undertaking security and privacy policies

g) Check data ownership and how data can be permanently deleted

h) Beware of “bundled consent” which signs you up for other unknown or unnecessarily services

i) Beware of “secondary uses” of your account information or services without your knowledge or consent

j) Know the exit process

3. Access Controls

k) Use stronger authentication means whenever possible

l) Choose different passwords for different user accounts

m) Change passwords periodically

n) Delete accounts or change passwords when there are staff changes

4. Data Protection

o) Think twice when storing sensitive data; assess the impact if data is exposed

p) Store sensitive data only if it is absolutely essential and that you have additional protection measures

q) Make sure only intended recipients can have access to your shared sensitive data

r) Use encryption when storing and transmitting whenever possible

5. Cloud Administration

s) Establish simple easy to understand cloud usage policies or rules for your staff to follow

t) Appoint a suitable staff as the cloud service administrator

u) Provide basic security awareness training for staff using the cloud service

v) Protect devices used to access the cloud

6. Service Continuity

w) Evaluate potential damage when service is unavailable

x) Develop business continuity plan and contingency plan if service or data is not available

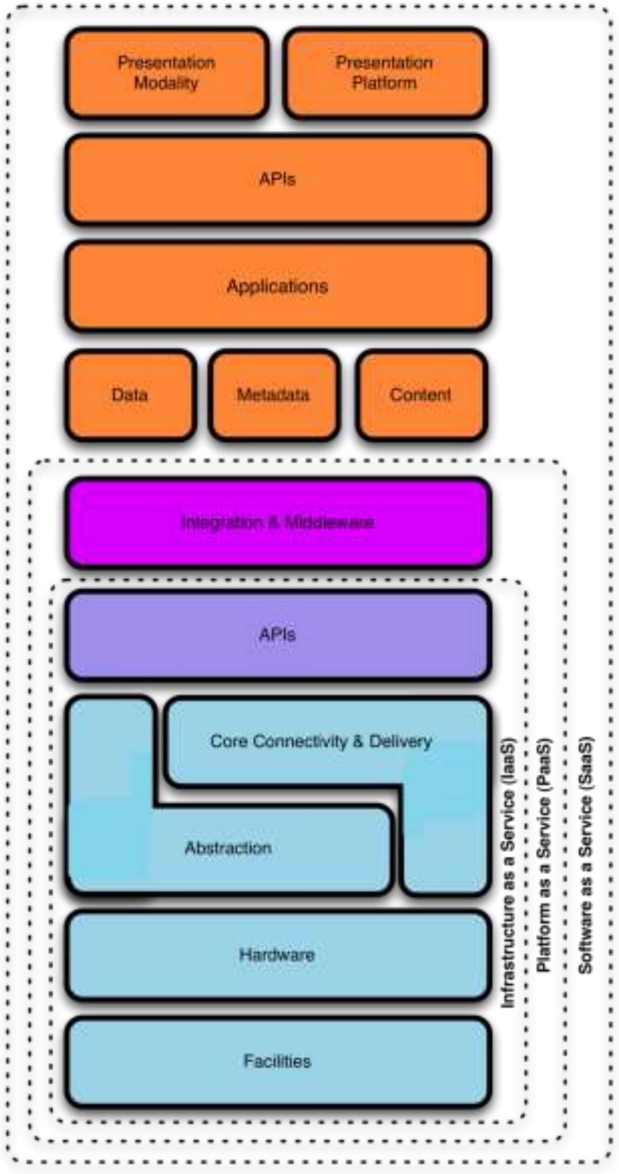
y) Maintain local backup copy of your important data stored in the cloud service

z) Prepare exit strategy to transfer data back to the company

How do we build the "Trusted Cloud"?

How CSA can support us?

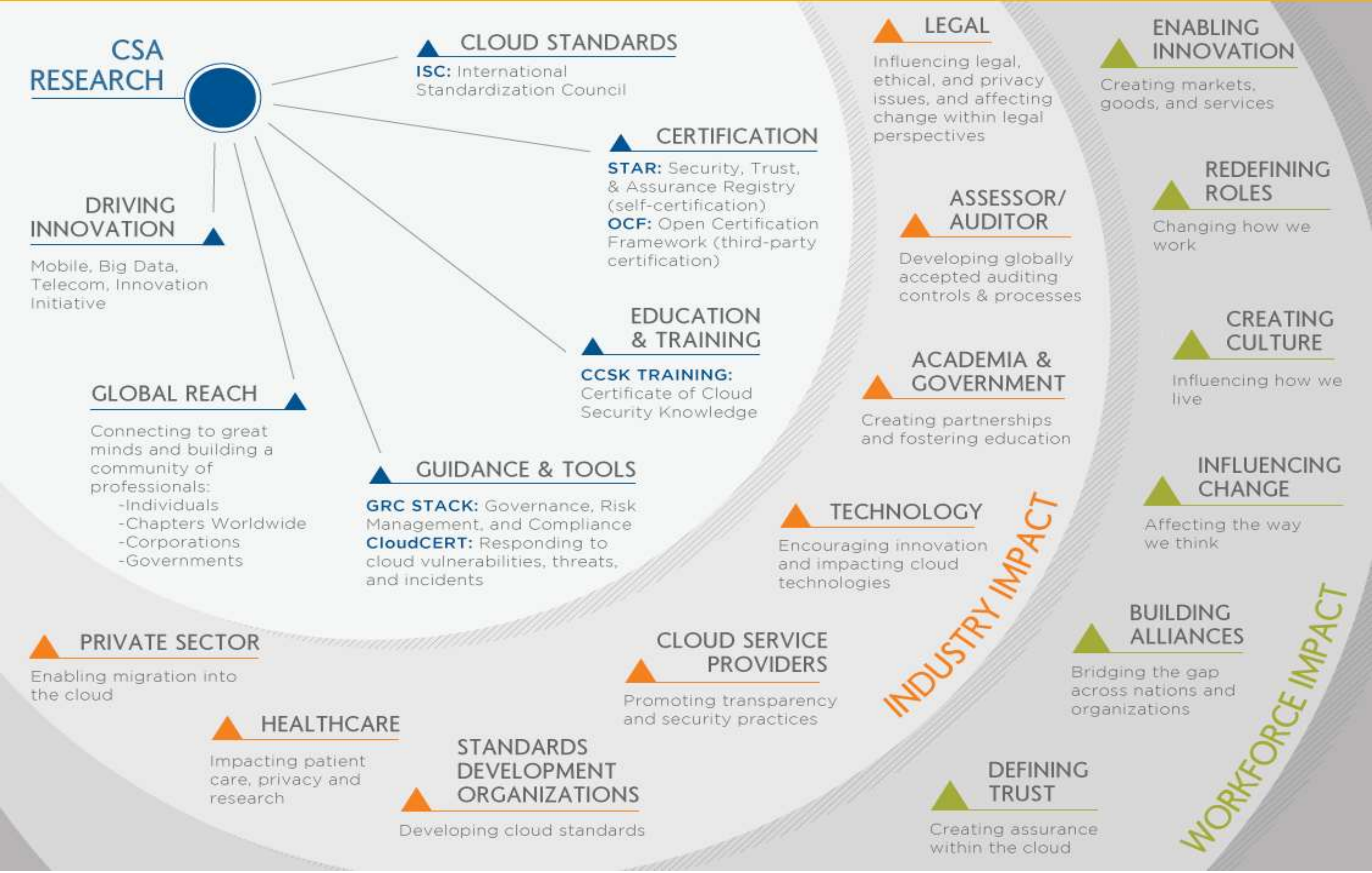
- 4 main areas
  - Research
  - Education
  - Certification
  - Collaborations



CSA RESEARCH – THE DOOR TO THE CLOUD+SECURITY UNIVERSE

AGILITY – COMMUNITY - MERITOCRACY

IMPACT OF CSA RESEARCH



CSA RESEARCH

CLOUD STANDARDS

ISC: International Standardization Council

CERTIFICATION

STAR: Security, Trust, & Assurance Registry (self-certification)
OCF: Open Certification Framework (third-party certification)

EDUCATION & TRAINING

CCSK TRAINING: Certificate of Cloud Security Knowledge

GUIDANCE & TOOLS

GRC STACK: Governance, Risk Management, and Compliance
CloudCERT: Responding to cloud vulnerabilities, threats, and incidents

GLOBAL REACH

Connecting to great minds and building a community of professionals:
- Individuals
- Chapters Worldwide
- Corporations
- Governments

DRIVING INNOVATION

Mobile, Big Data, Telecom, Innovation Initiative

INDUSTRY IMPACT

LEGAL

Influencing legal, ethical, and privacy issues, and affecting change within legal perspectives

ASSESSOR/ AUDITOR

Developing globally accepted auditing controls & processes

ACADEMIA & GOVERNMENT

Creating partnerships and fostering education

TECHNOLOGY

Encouraging innovation and impacting cloud technologies

CLOUD SERVICE PROVIDERS

Promoting transparency and security practices

STANDARDS DEVELOPMENT ORGANIZATIONS

Developing cloud standards

HEALTHCARE

Impacting patient care, privacy and research

PRIVATE SECTOR

Enabling migration into the cloud

WORKFORCE IMPACT

ENABLING INNOVATION

Creating markets, goods, and services

REDEFINING ROLES

Changing how we work

CREATING CULTURE

Influencing how we live

INFLUENCING CHANGE

Affecting the way we think

BUILDING ALLIANCES

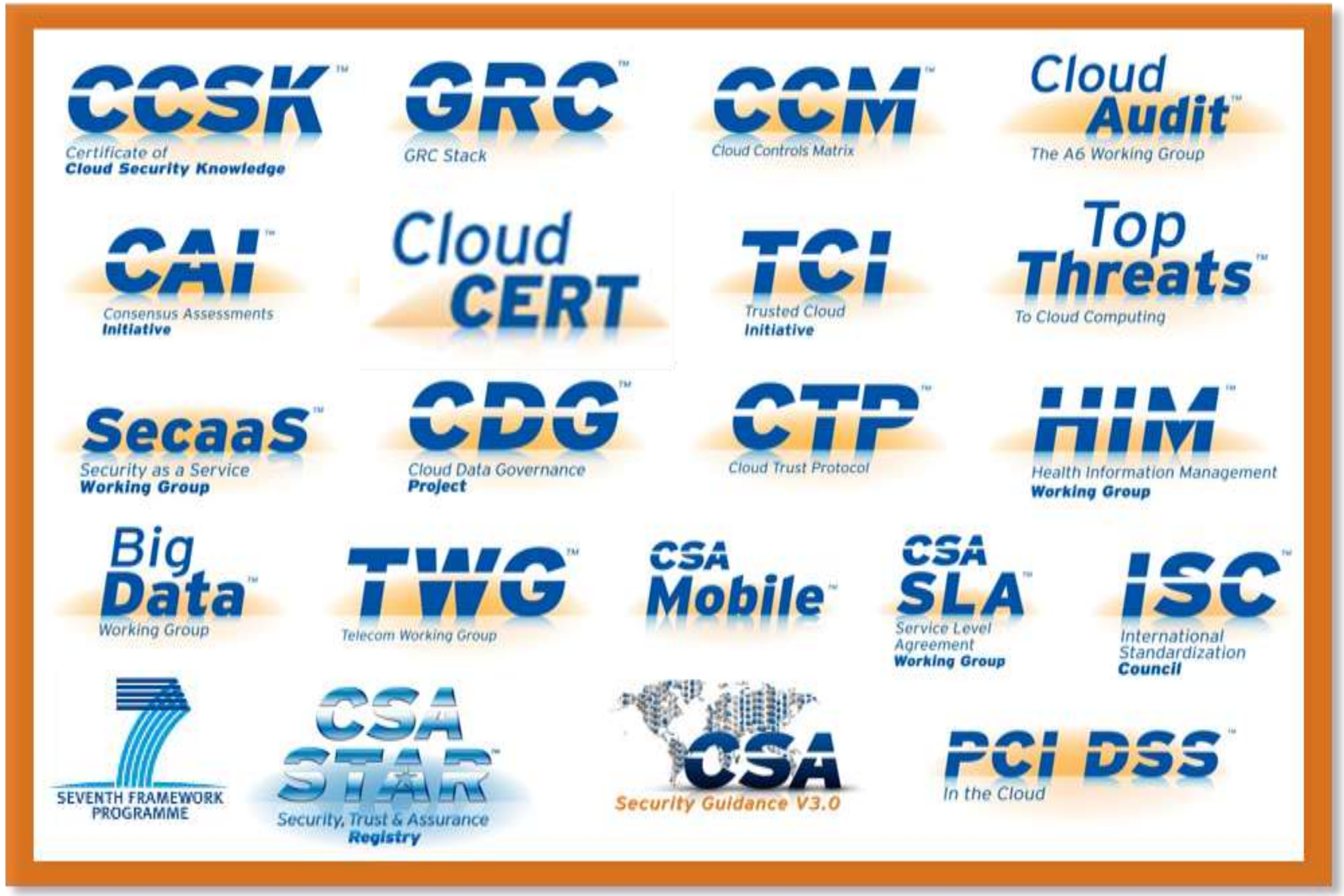
Bridging the gap across nations and organizations

DEFINING TRUST

Creating assurance within the cloud

Research portfolio

- Our research includes fundamental projects needed to define and implement trust within the future of information technology
- CSA continues to be aggressive in producing critical research, education and tools
- 22 Active Work Groups and 10 in the pipeline


CCSK Certificate of Cloud Security Knowledge
GRC GRC Stack
CCM Cloud Controls Matrix
Cloud Audit The A6 Working Group
CAI Consensus Assessments Initiative
Cloud CERT
TCI Trusted Cloud Initiative
Top Threats To Cloud Computing
SecaaS Security as a Service Working Group
CDG Cloud Data Governance Project
CTP Cloud Trust Protocol
HIM Health Information Management Working Group
Big Data Working Group
TWG Telecom Working Group
CSA Mobile
CSA SLA Service Level Agreement Working Group
ISC International Standardization Council
7 SEVENTH FRAMEWORK PROGRAMME
CSA STAR Security, Trust & Assurance Registry
CSA Security Guidance V3.0
PCI DSS In the Cloud

AGILITY

COMMUNITY

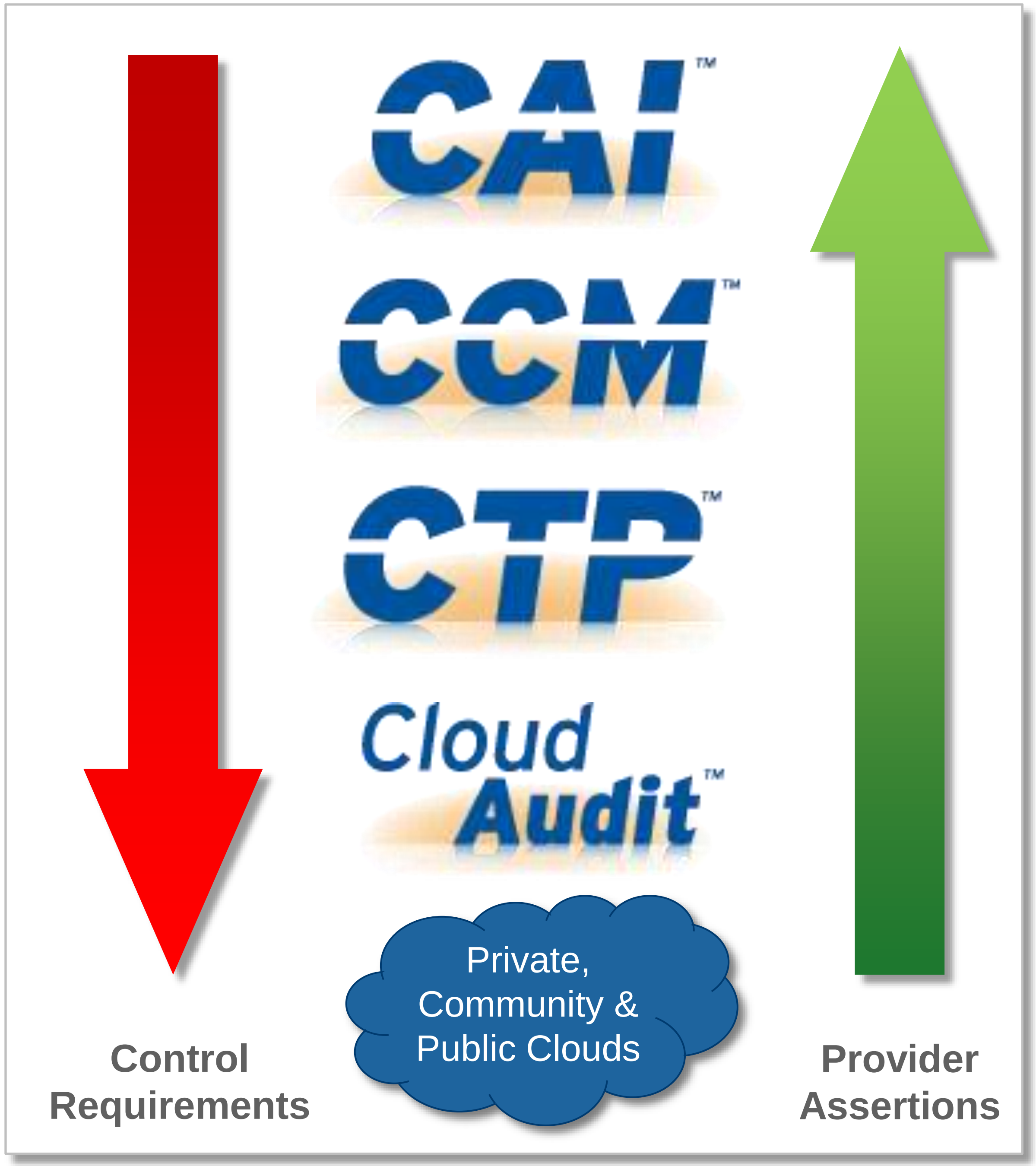
MERITOCRACY

CSA cloud security alliance

RESEARCH PHILOSOPHY

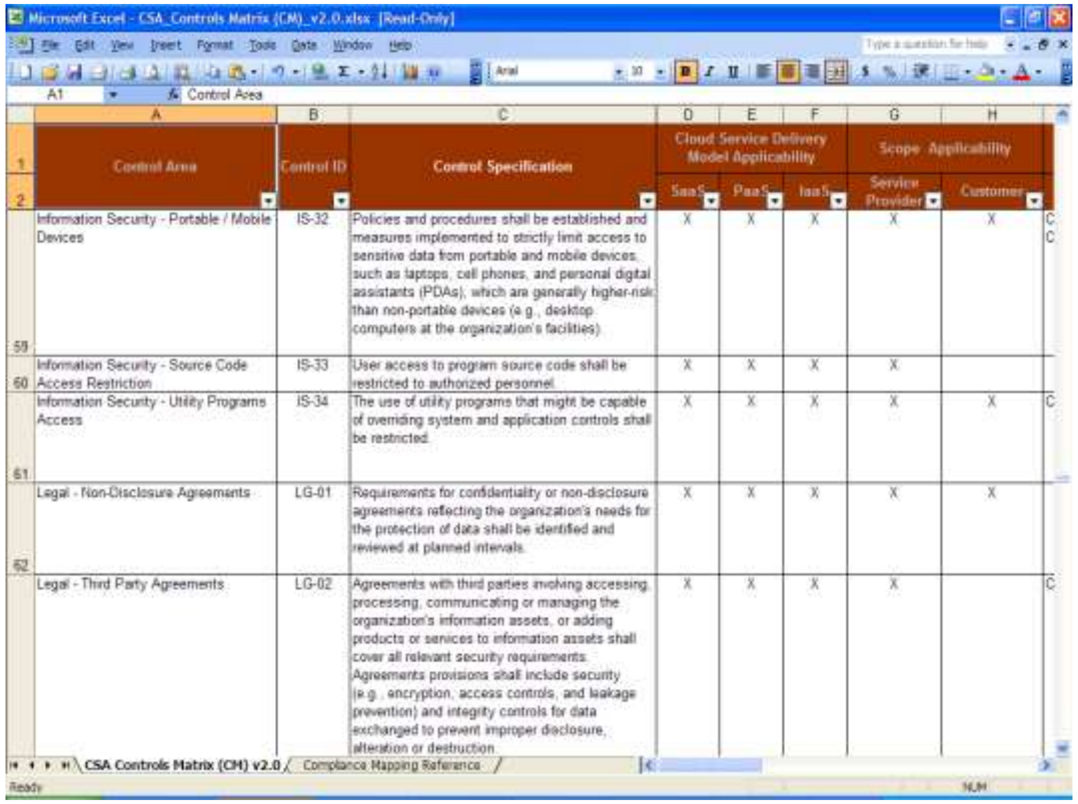
CSA GRC Stack

- Family of 4 research projects
  - Cloud Controls Matrix
  - Consensus Assessments Initiative
  - Cloud Audit
  - Cloud Trust Protocol
- Tools for governance, risk and compliance management



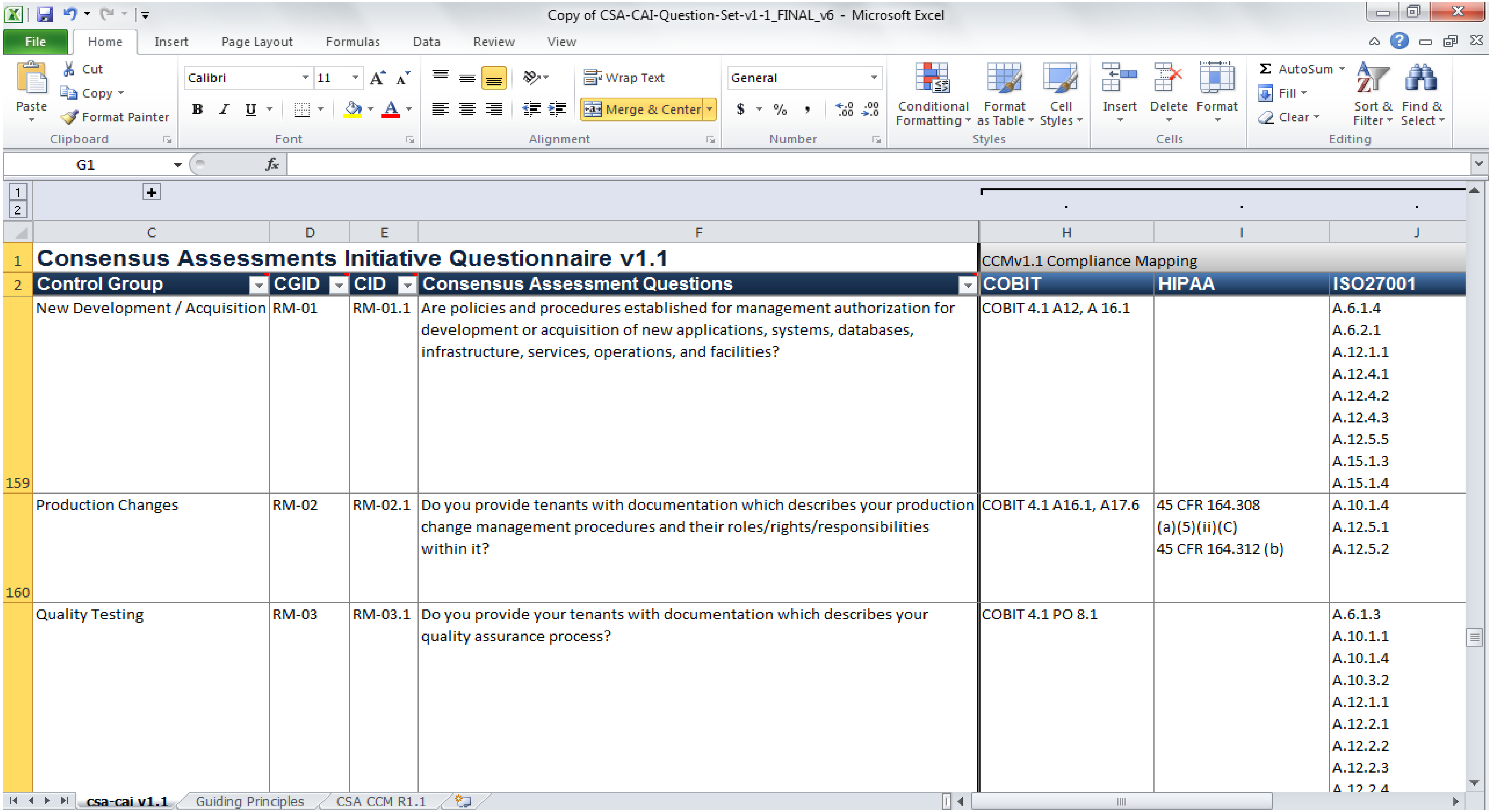
Cloud Controls Matrix Tool

- Controls derived from guidance
- Mapped to familiar frameworks: ISO 27001, COBIT, PCI, HIPAA, FISMA, FedRAMP, etc.
- Rated as applicable to S-P-I
- Customer vs. Provider role
- Help bridge the “cloud gap” for IT & IT auditors


Microsoft Excel - CSA_Controls Matrix (CM)_v2.0.xlsx [Read-Only]
File Edit View Insert Format Tools Data Window Help
Type a question for help
Arial
10
A1
Control Area
CSA Controls Matrix (CM) v2.0
Compliance Mapping Reference
Ready
NUM

	A	B	C	D	E	F	G	H	
1	Control Area	Control ID	Control Specification	Cloud Service Delivery Model Applicability			Scope Applicability		
2				SaaS	PaaS	IaaS	Service Provider	Customer	
59	Information Security - Portable / Mobile Devices	IS-32	Policies and procedures shall be established and measures implemented to strictly limit access to sensitive data from portable and mobile devices, such as laptops, cell phones, and personal digital assistants (PDAs), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization's facilities).	X	X	X	X	X	C C
60	Information Security - Source Code Access Restriction	IS-33	User access to program source code shall be restricted to authorized personnel.	X	X	X	X		
61	Information Security - Utility Programs Access	IS-34	The use of utility programs that might be capable of overriding system and application controls shall be restricted.	X	X	X	X	X	C
62	Legal - Non-Disclosure Agreements	LG-01	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of data shall be identified and reviewed at planned intervals.	X	X	X	X	X	
	Legal - Third Party Agreements	LG-02	Agreements with third parties involving accessing, processing, communicating or managing the organization's information assets, or adding products or services to information assets shall cover all relevant security requirements. Agreements provisions shall include security (e.g., encryption, access controls, and leakage prevention) and integrity controls for data exchanged to prevent improper disclosure, alteration or destruction.	X	X	X	X		C

The CAIQ Questionnaire



Copy of CSA-CAI-Question-Set-v1-1_FINAL_v6 - Microsoft Excel

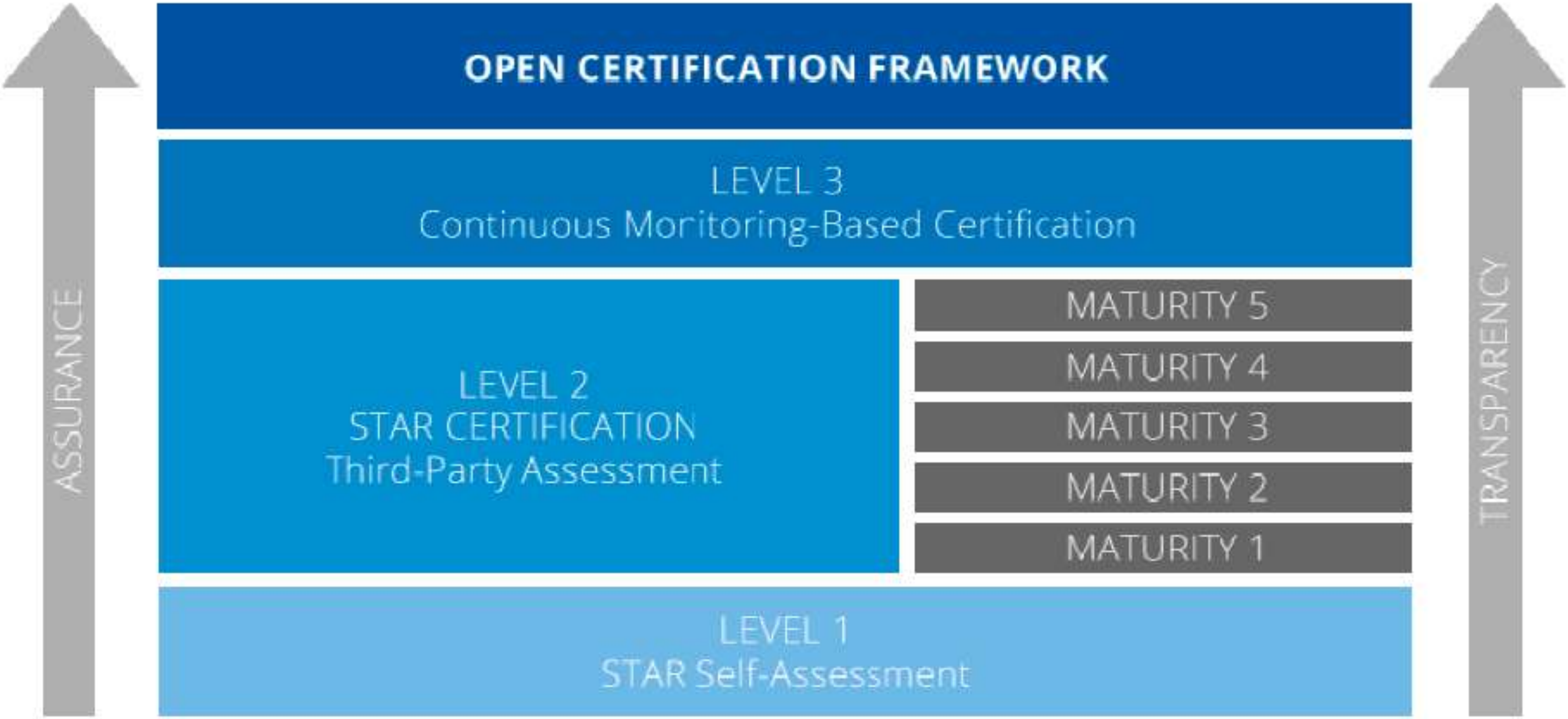
	C	D	E	F	H	I	J
1	Consensus Assessments Initiative Questionnaire v1.1				CCMv1.1 Compliance Mapping		
2	Control Group	CGID	CID	Consensus Assessment Questions	COBIT	HIPAA	ISO27001
159	New Development / Acquisition	RM-01	RM-01.1	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations, and facilities?	COBIT 4.1 A12, A 16.1		A.6.1.4 A.6.2.1 A.12.1.1 A.12.4.1 A.12.4.2 A.12.4.3 A.12.5.5 A.15.1.3 A.15.1.4
160	Production Changes	RM-02	RM-02.1	Do you provide tenants with documentation which describes your production change management procedures and their roles/rights/responsibilities within it?	COBIT 4.1 A16.1, A17.6	45 CFR 164.308 (a)(5)(ii)(C) 45 CFR 164.312 (b)	A.10.1.4 A.12.5.1 A.12.5.2
	Quality Testing	RM-03	RM-03.1	Do you provide your tenants with documentation which describes your quality assurance process?	COBIT 4.1 PO 8.1		A.6.1.3 A.10.1.1 A.10.1.4 A.10.3.2 A.12.1.1 A.12.2.1 A.12.2.2 A.12.2.3 A.12.2.4

cloud security alliance℠

CAIQ Questionnaire

- Control Group, Control Group ID (CGID) and Control Identifier (CID) all map the CAIQ question being asked directly to the CCM control that is being addressed.
- Relevant compliance and standards are mapped line by line to the CAIQ, which, in turn, also map to the CCM. The CAIQ v1.1 maps to the following compliance areas – HIPPA, ISO 27001, COBIT, SP800_53, FedRAMP, PCI_DSS, BITS and GAPP. V1.2 will additionally include mappings to Jericho Forum and NERC CIP.
- Each question can be answered by a provider with a yes or no answer.

CSA Open Certification Framework



EDUCATION

Training courses available today

- CCSK Basic

  One day course to enable student to pass CCSK

- CCSK Plus

  Two day course includes practical cloud lab work

- CCSK Train-the-Trainer

  Three day course including CCSK Plus

- GRC Stack Training

  Additional one day course to use GRC Stack components

- PCI/DSS In the Cloud

  Additional one day course focusing on achieving PCI compliance in cloud computing

- http://cloudsecurityalliance.org/education/training/

New courses to be developed in the CoE in Singapore

- CCSK for IT & Security Architects
  - Whitepaper: Security best practices for security architecture in the cloud derived from CSA Domain 1, Trusted Cloud Initiative Reference Architecture model and new materials.
  - Courseware: Development of 3 day courseware derived from above whitepaper and other CSA materials.
- CCSK for Software Developers
  - Whitepaper: Security best practices for software development in the cloud and recommended industry curriculum.
  - Courseware: Development of 3 day courseware derived from above whitepaper and other CSA materials.
- CCSK for Cloud Auditing/Assurance (GRC Stack)
  - Whitepaper: Security best practices for assurance in the cloud derived from CSA Guidance 3 and components of the GRC Stack research projects.
  - Courseware: Development of 3 day courseware derived from existing GRC Stack courseware, above whitepaper and other CSA materials.

CERTIFICATION

http://cloudsecurityalliance.org/education/

Introducing Certificate of Cloud Security Knowledge (CCSK)

- The industry’s first user certification program for secure cloud computing
- Based on CSA research framework, specifically the Security Guidance for Critical Area of Focus in Cloud Computing
- Designed to ensure that a broad range of professionals with responsibility related to cloud computing have a demonstrated awareness of the security threats and best practices for securing the cloud

CCSK™
Certificate of
Cloud Security Knowledge

Certificate of Cloud Security Knowledge (CCSK)

CCSK™
Certificate of
Cloud Security Knowledge

- Benchmark of cloud security competency
- Measures mastery of CSA guidance and ENISA cloud risks whitepaper
- Understand cloud issues
- Look for the CCSKs at cloud providers, consulting partners
- Online web-based examination
- www.cloudsecurityalliance.org/certifyme

COLLABORATIONS

http://cloudsecurityalliance.org

How do you get involved?

Get involved

Learn how you can participate in Cloud Security Alliance's goals to promote the use of best practices for providing security assurance within Cloud Computing

http://www.linkedin.com/groups?gid=1864210
https://cloudsecurityalliance.org/get-involved/

http://www.linkedin.com/groups?gid=4069005 (HK&M)

New Research Ideas

Submit Your Research Ideas

- Do you have an idea for a research project on a cloud security topic? If so, please take the time to describe your concept. Ideas are monitored by the CSA research team, who will review your proposal and respond to you with feedback.

https://cloudsecurityalliance.org/research/, the Submit Ideas tab

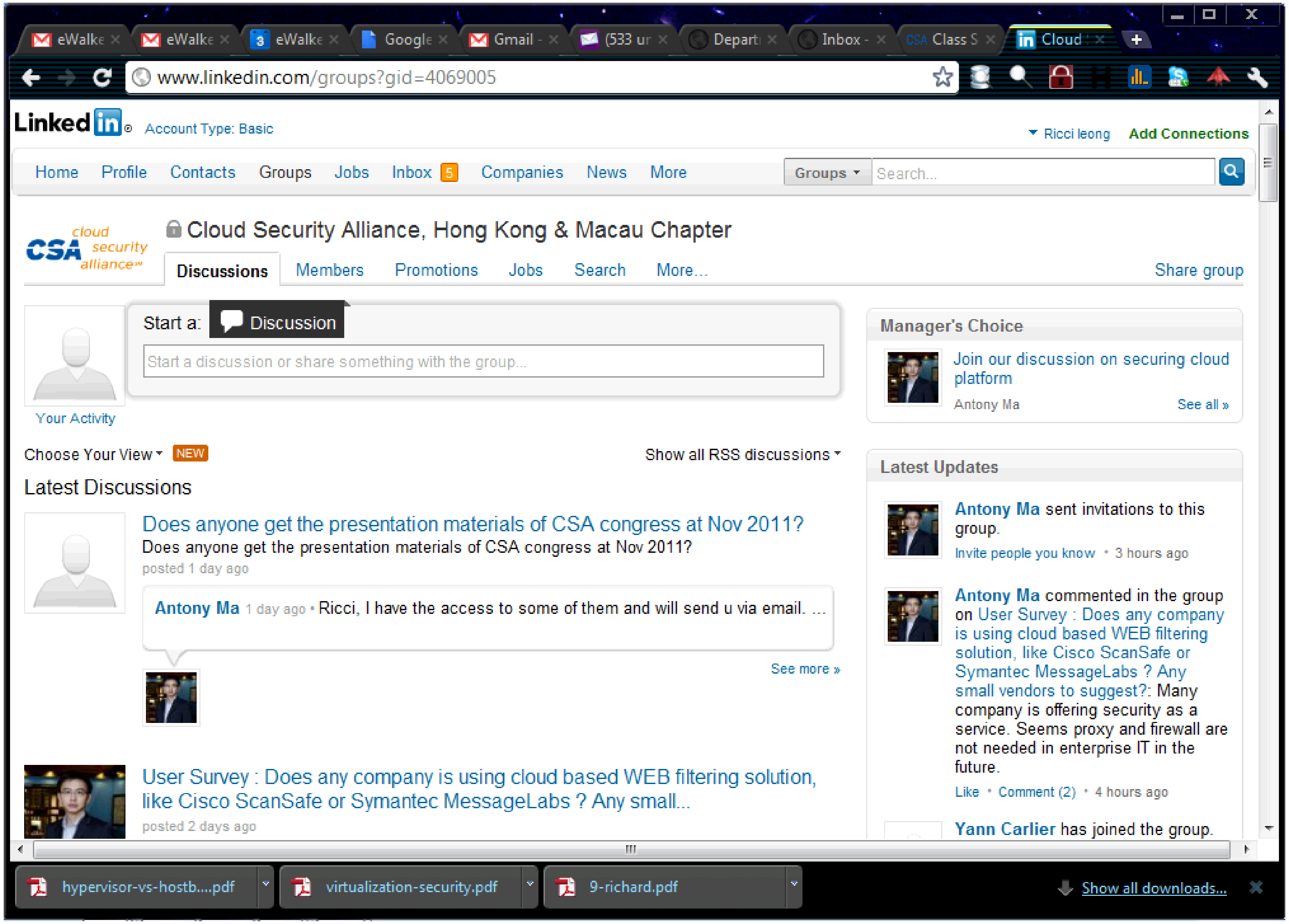
CSA Library

Contribute to the CSA library

- The Cloud Security Alliance is a community non-profit which is driven by its members. Have a white paper or information on a cloud security product you want to contribute?

https://cloudsecurityalliance.org/education/white-papers-and-educational-material/

Cloud Security Alliance (HK&M)



Cloud Security Alliance, Hong Kong & Macau Chapter

Start a: Discussion

Start a discussion or share something with the group...

Latest Discussions

Does anyone get the presentation materials of CSA congress at Nov 2011?
Does anyone get the presentation materials of CSA congress at Nov 2011?
posted 1 day ago

Antony Ma 1 day ago • Ricci, I have the access to some of them and will send u via email. ...

See more »

User Survey : Does any company is using cloud based WEB filtering solution, like Cisco ScanSafe or Symantec MessageLabs ? Any small...
posted 2 days ago

Manager's Choice

Join our discussion on securing cloud platform
Antony Ma
See all »

Latest Updates

Antony Ma sent invitations to this group.
Invite people you know • 3 hours ago

Antony Ma commented in the group on User Survey : Does any company is using cloud based WEB filtering solution, like Cisco ScanSafe or Symantec MessageLabs ? Any small vendors to suggest?: Many company is offering security as a service. Seems proxy and firewall are not needed in enterprise IT in the future.
Like • Comment (2) • 4 hours ago

Yann Carlier has joined the group.

http://www.linkedin.com/groups?gid=4069005 (HK&M)

Let's Get Started!