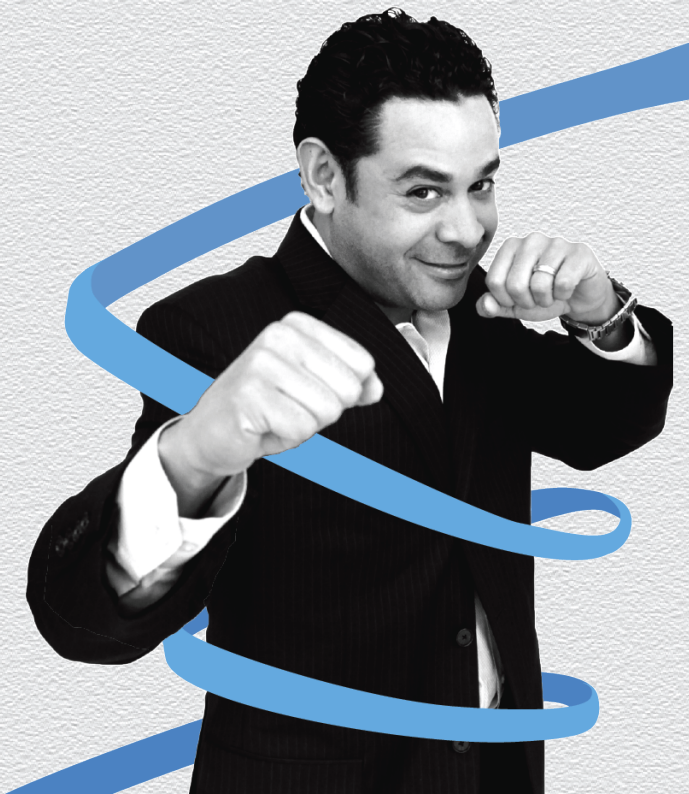
RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

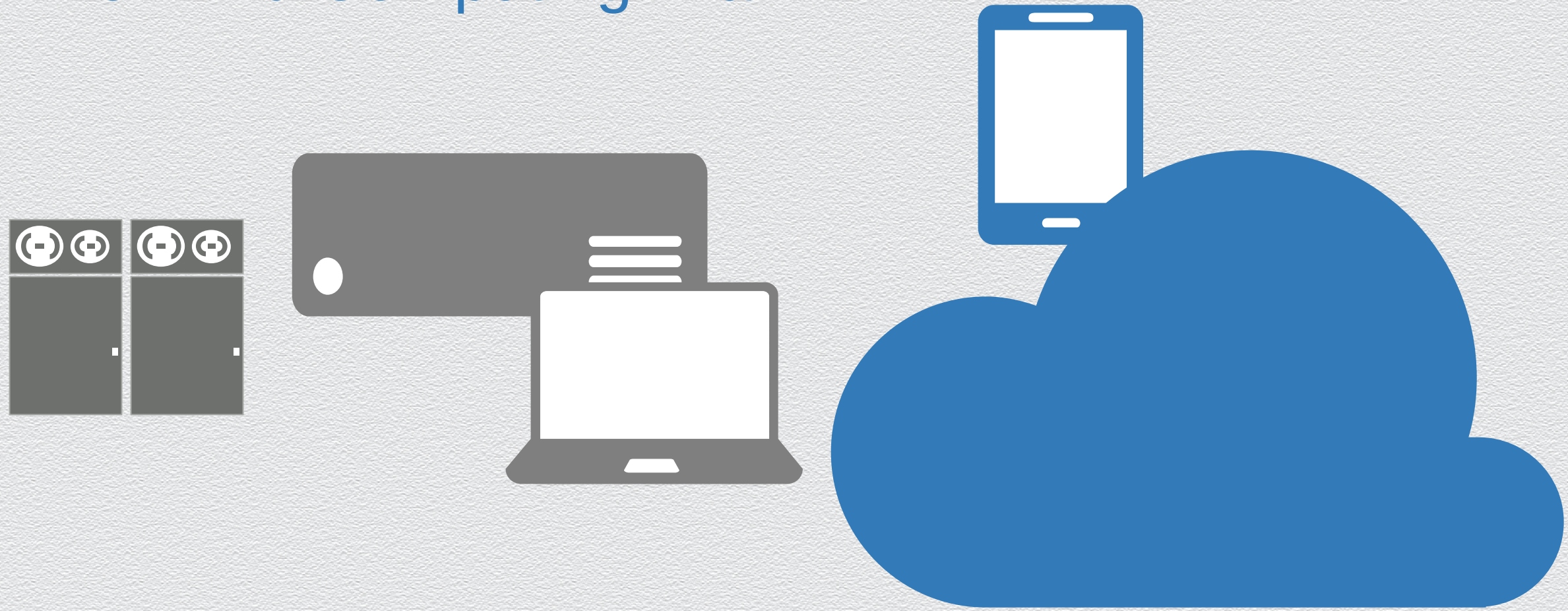
Public Cloud Security:
Surviving in a Hostile Multitenant Environment

SESSION ID: EXP-R01



Mark Russinovich
Technical Fellow
Windows Azure, Microsoft
@markrussinovich

The Third Computing Era



Security Could Hamper the Transformational Benefits of Cloud Computing

Microsoft

#RSAC

RSACONFERENCE2014

JOURNAL OF ACCOUNTANCY

HOME | NEWS | CURRENT ISSUE | VIDEO | TOPICS

Home > News > Survey: Data security concerns soar as more CPA firms access cloud

TECHNOLOGY

Survey: I
access clo

BY JEFF DREW
NOVEMBER 20, 2013

Concerns about
continues to inc
subsidiary.

January 15th, 2014, 15:43 GMT · By Gabriela Vatu

Cloud Adoption Hindered by S
Survey Reveals

**Cloud services continue to face perception pro
have security concerns when it comes to these**

INTERNAP

ENLARGE

According to a global survey from the Internap Netw
currently trusting cloud services with their data hav

The survey also reveals that there's a significant difference in public cloud infrastructure concerns between the companies that are currently using such services and those that have no immediate plans to make the switch from traditional data storage services.

For the poll, nearly 250 global Internet infrastructure decision makers were interviewed. These are part of a range of industries including software and Internet hosting and

Op
oper

Forbes

New Posts | Popular (The WhatsApp Billiona) | Lists (The Business Of Nasc) | Vide (Olym)

Louis Columbus, Contributor
I cover CRM, Cloud Computing, ERP and Enterprise Software
+ Follow (326)

TECH | 8/13/2013 @ 3:07PM | 7,835 views

IDG Cloud Computing Survey: Security, Integration Challenge Growth

10 comments, 10 called-out + Comment Now + Follow Comments

IDG Enterprise recently published Cloud Computing: Key Trends and Future Effects Report, showing how enterprises continue to struggle with security, integration and governance while finding immediate

76 Share
270 Tweet
226

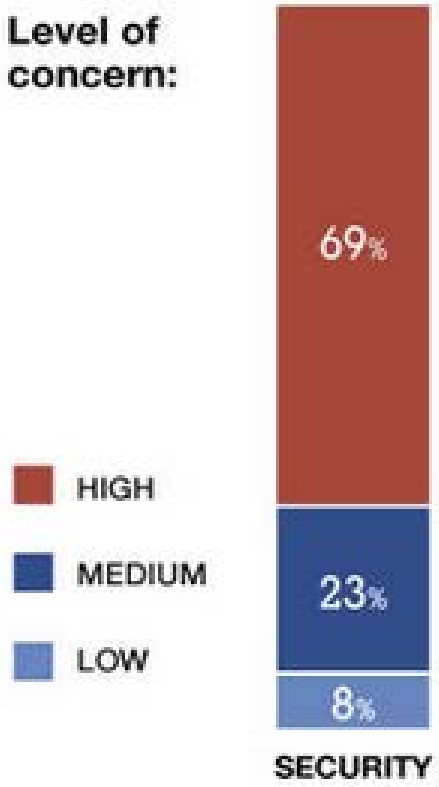
Microsoft

#RSAC

RSACONFERENCE2014

Concerns about public cloud hosting

Concerns about security and compliance with PCI and other standards in public cloud hosting environments remain high.

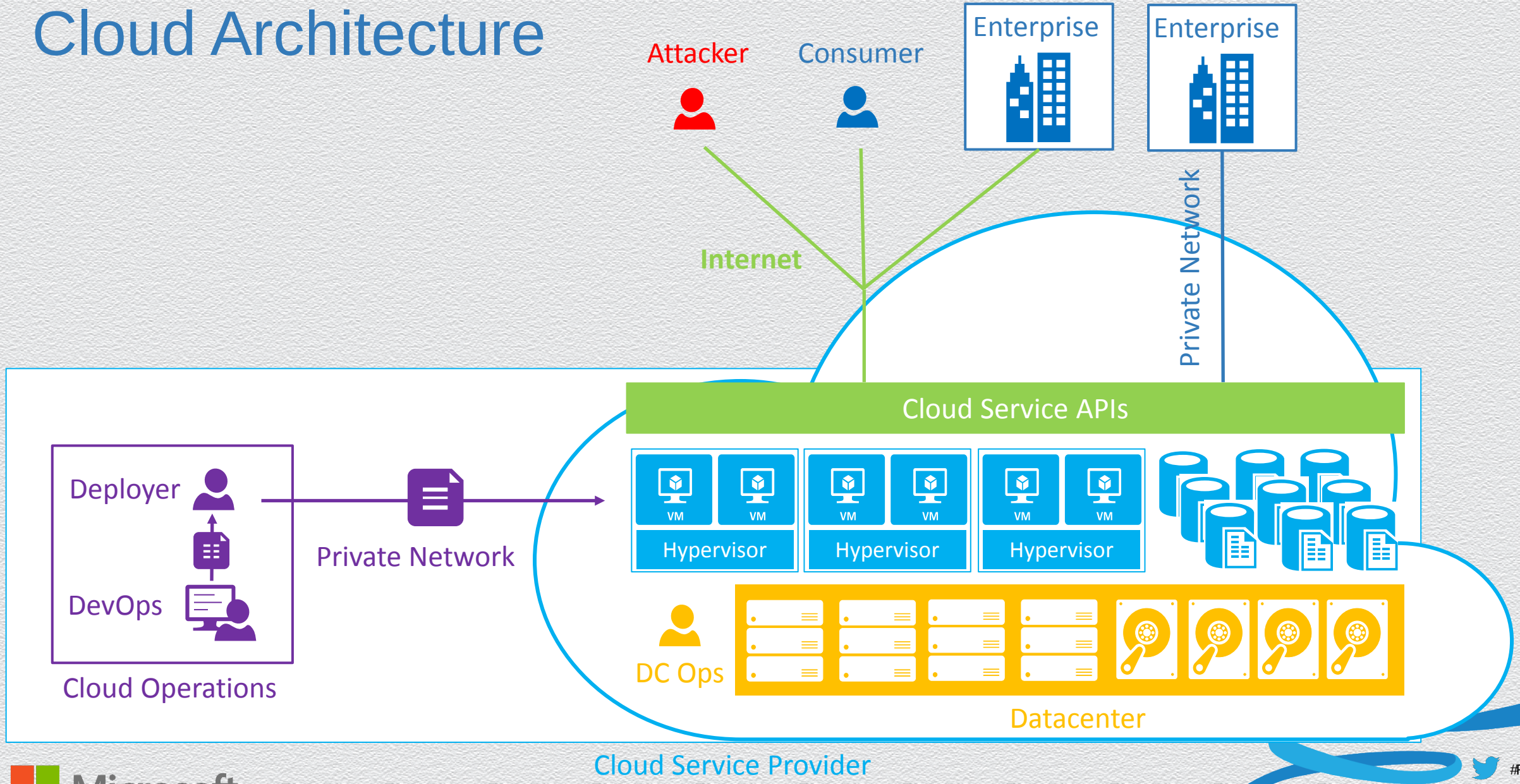


Source: 451 Research, Dec 2012

Goals of this Session

- Identify threats
- Discuss risk
- Explore mitigations

Cloud Architecture



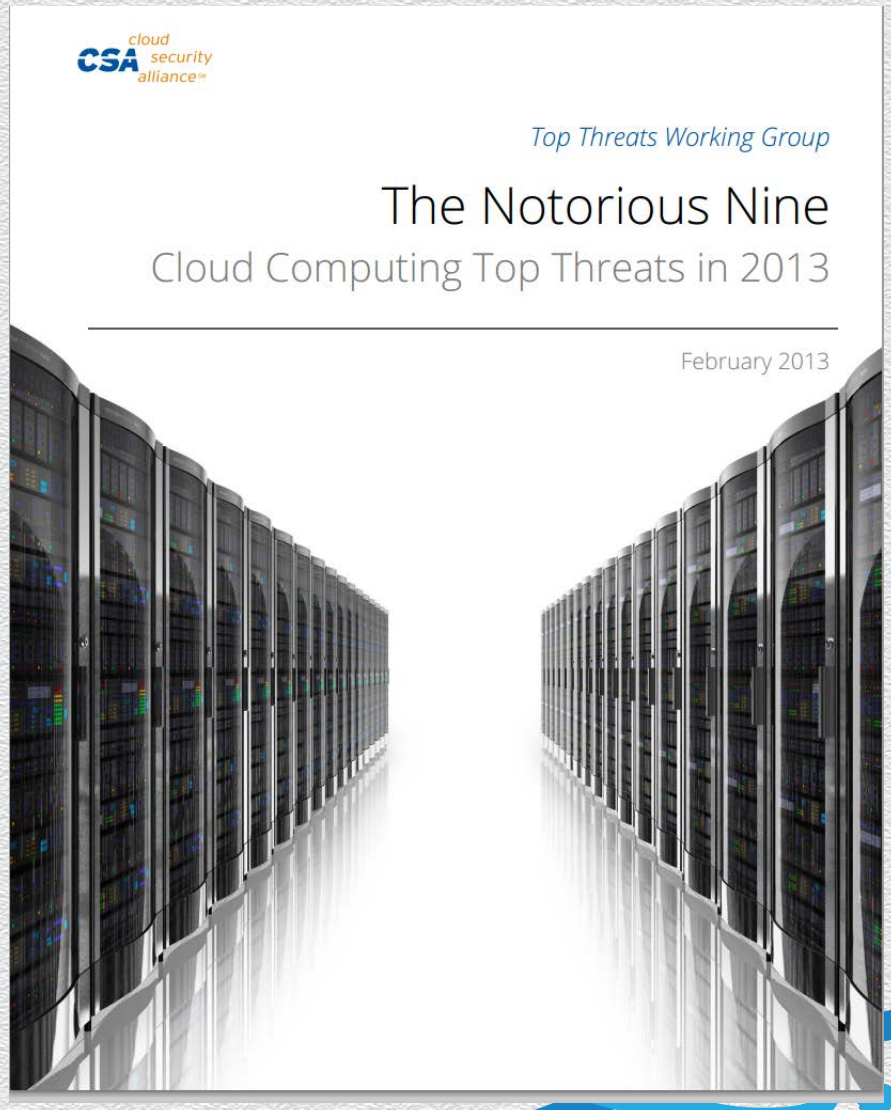
Microsoft

#RSAC

RSACONFERENCE2014

The Cloud Security Alliance "Notorious Nine"

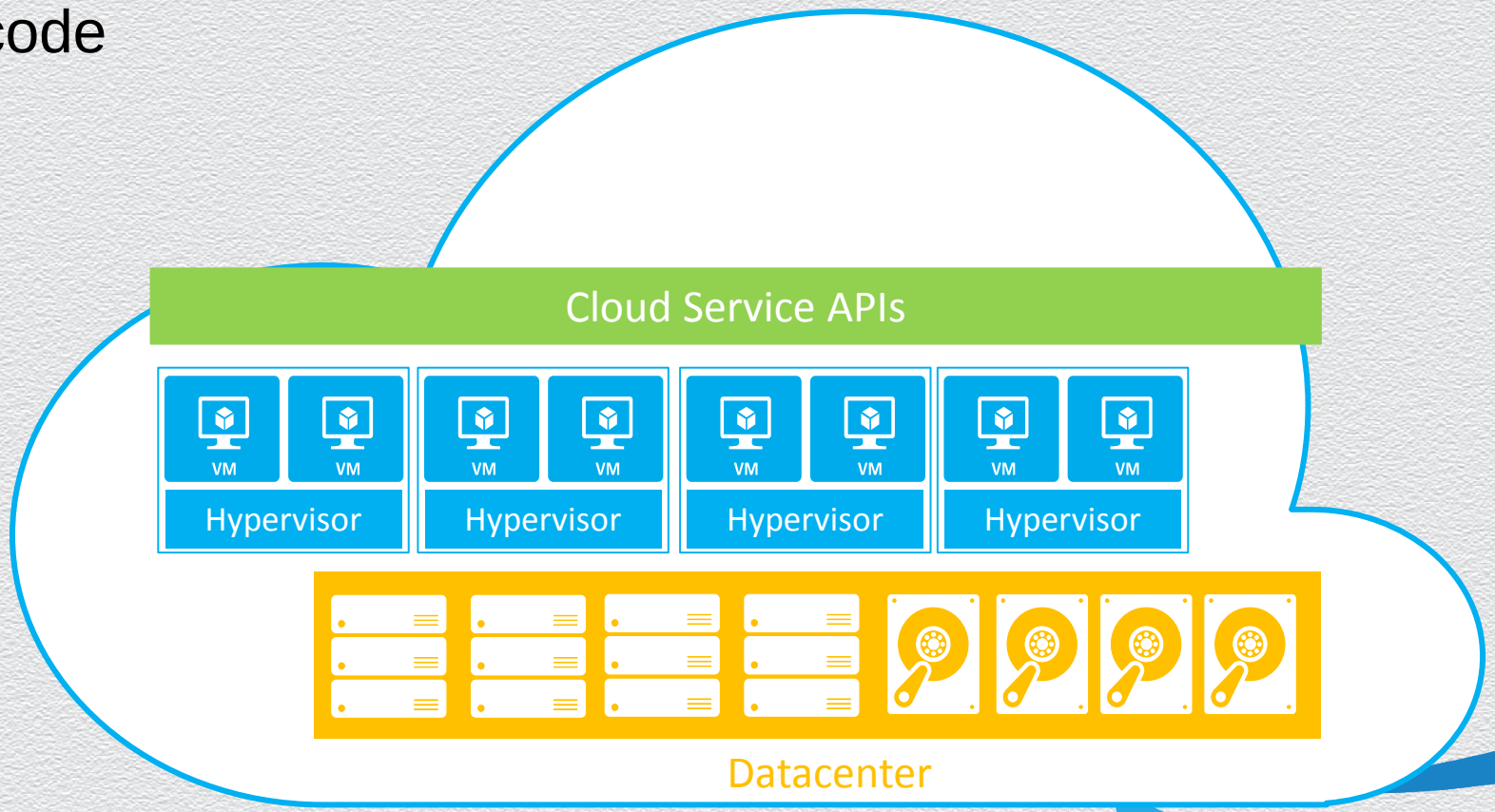
- CSA periodically surveys industry experts to identify top cloud computing threats
- First report published in 2010
  - Seven top threats
- Most recent report published in February 2013
  - Nine top threats
  - So close to a top ten list…



https://cloudsecurityalliance.org/research/top-threats/

10. Shared Technology Issues: Exposed Software

- Some shared code defines the surface area exposed to customers:
  - CPU firmware/microcode
  - Hypervisor
  - Web server
  - API support libraries
  - …

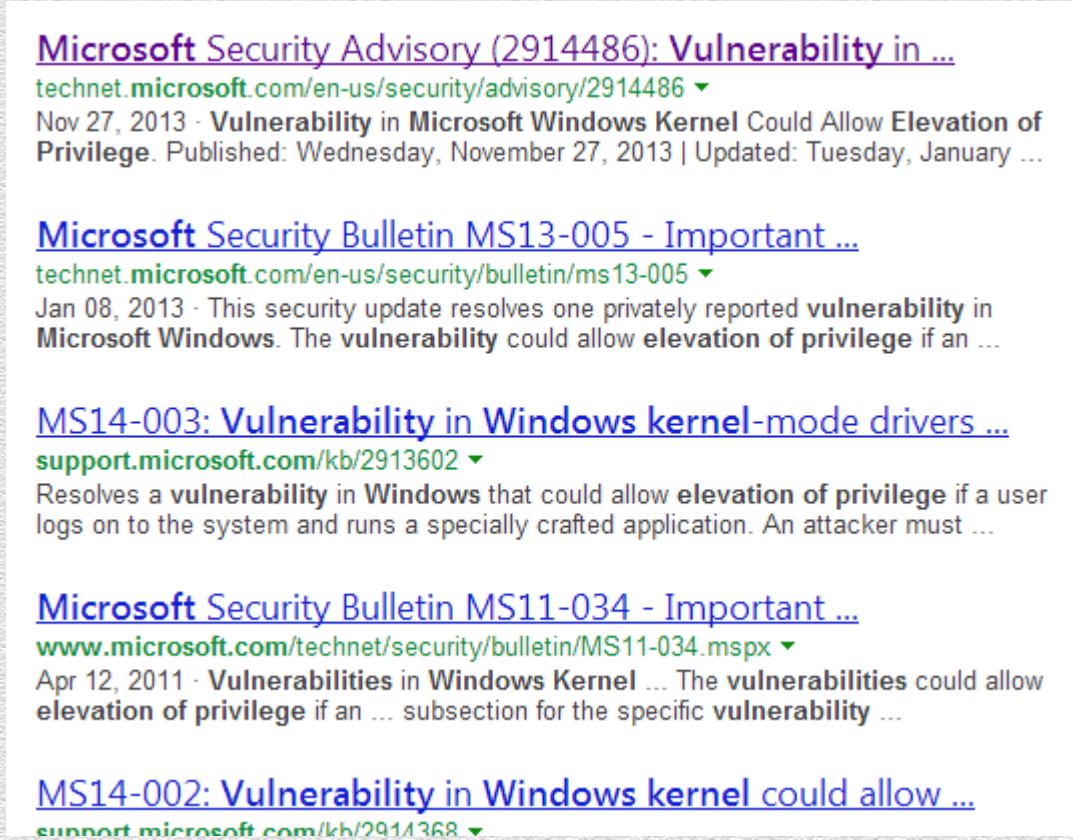


10. Shared Technology Issues

- What if there's a vulnerability?

10. Shared Technology Vulnerabilities: The Enterprise Approach

- Stability and security are balanced against each other
- Assumes infrastructure is accessible only by trusted actors
- Corporate and legal mechanisms for dealing with attackers



Enterprise Multi-tenancy

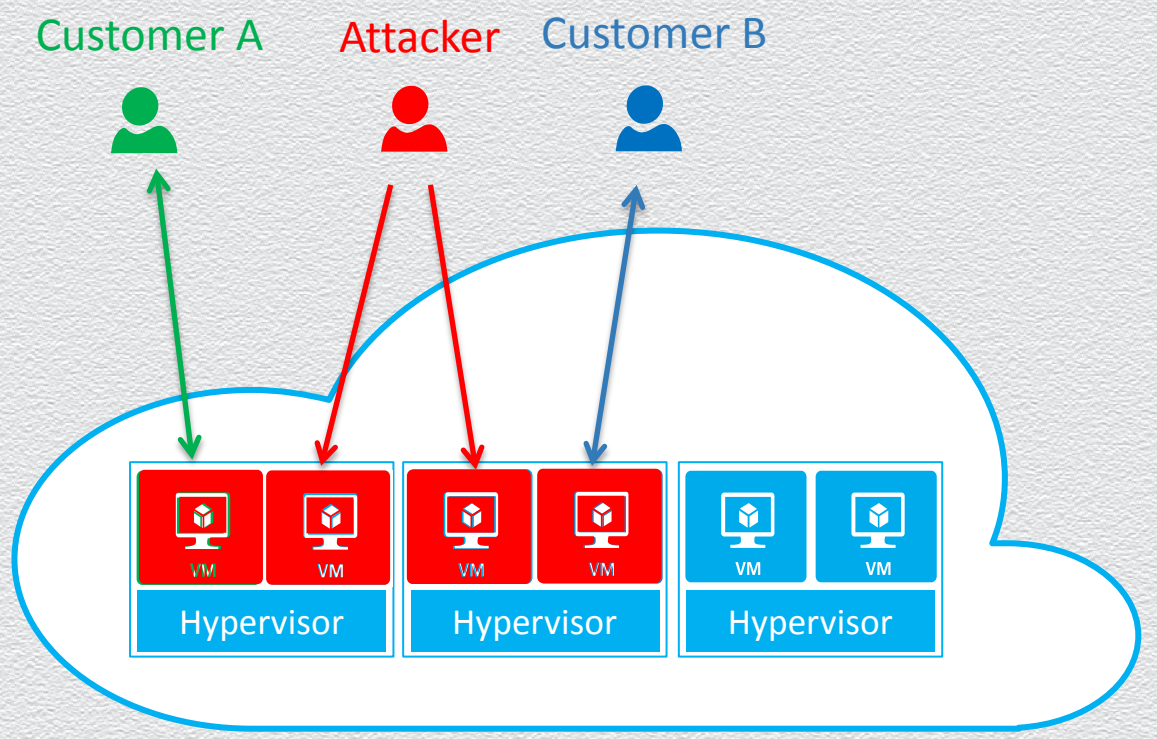
Microsoft

#RSAC

RSA CONFERENCE 2014

10. Shared Technology Vulnerabilities: The Cloud Risk

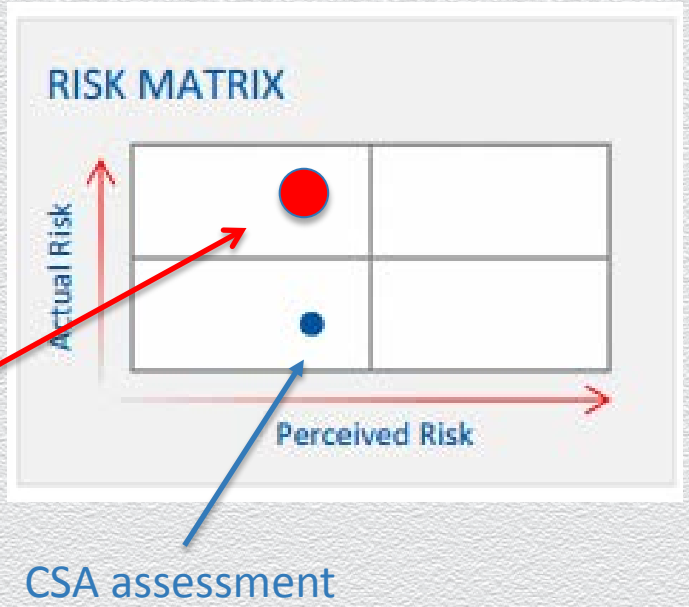
- A vulnerability in publically accessible software enables an attacker to puncture the cloud
  - Breach exposes data of other customers
  - Single incident can cause catastrophic loss of customer confidence
  - Customers (potential attackers) are anonymous and in diverse jurisdictions
- New bug classification: “Cloud Critical”



Hostile Multi-tenancy

10. Shared Technology Vulnerabilities: Bottom Line

- Enterprises and clouds are exposed to this risk
- Clouds are at higher risk of exploitation:
  - Data from many customers makes it a rich target
  - API surface is trivial to access
- Clouds are generally better at response:
  - Their business depends on it
  - Automated software deployment and patching required for cloud scale
  - Breach detection/mitigation necessary for preserving trust



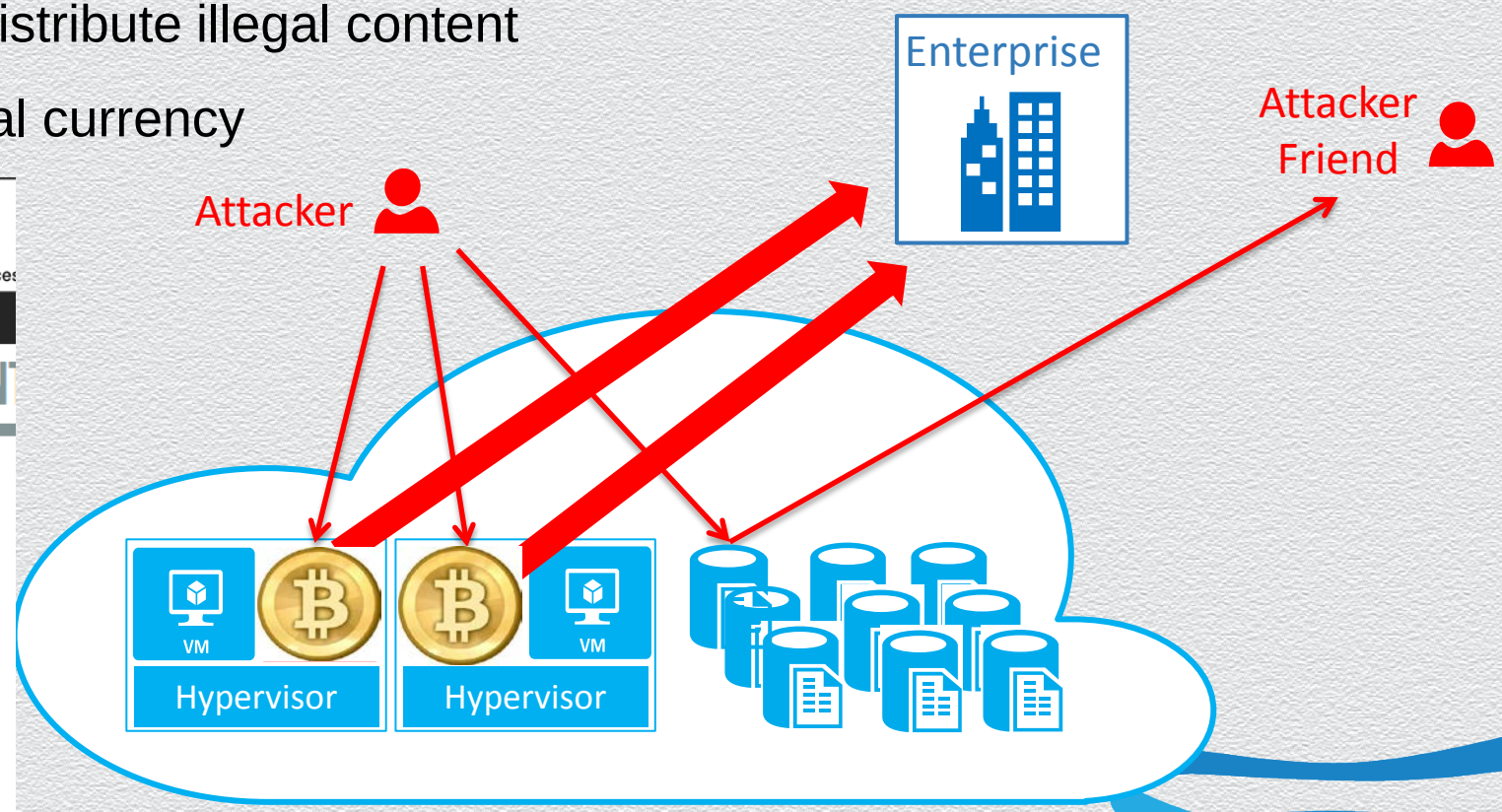
9. Insufficient Due Diligence

- Many companies are moving to the cloud and side-stepping IT processes:
  - IT management, auditing, forensics, and access control systems are designed for on-premises servers and applications
  - Shadow IT: when business units bypass IT to deploy applications and store data in the cloud
- Bottom line:
  - IT must determine how to enable business units while enforcing corporate governance
  - IT must lead responsible adoption – it's happening with or without them

Microsoft

8. Abuse of Cloud Services

- The agility and scale of the cloud is attractive to attackers, too
  - Use of compute as malware platform (Botmaster, DDOS platform)
  - Use of storage to store and distribute illegal content
  - Use of compute to mine digital currency



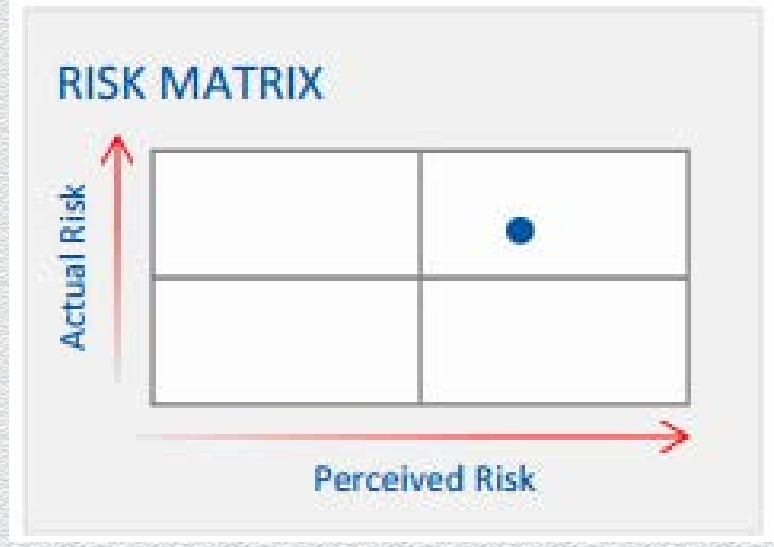
Microsoft

#RSAC

RSACONFERENCE2014

8. Abuse of Cloud Services: It's Happening

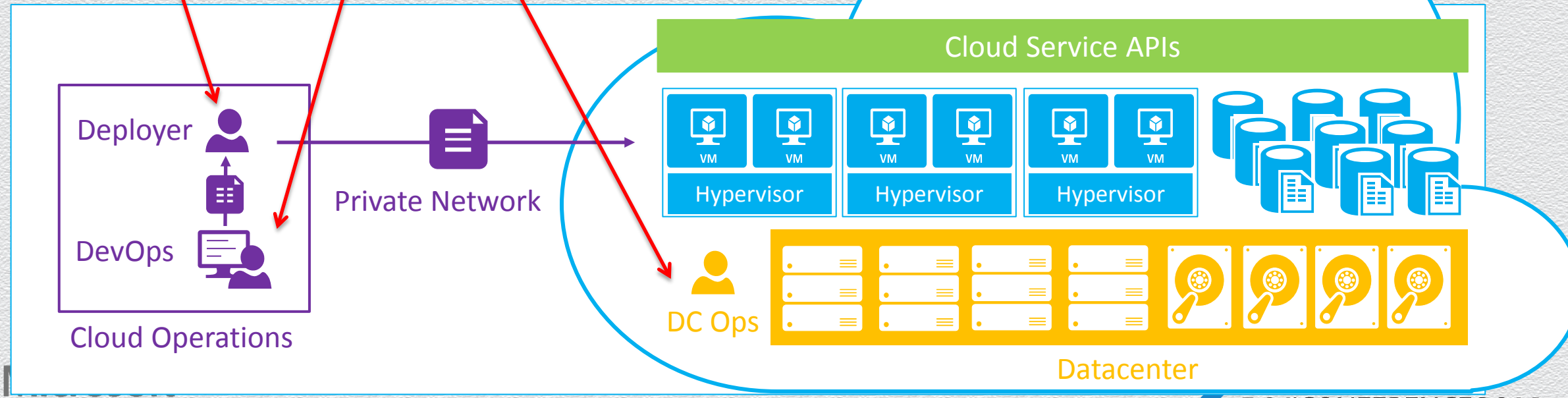
- Attackers can use cloud resources and remain anonymous
  - Free trial offers
  - Stolen credit cards
  - Hijacked accounts
- Bottom line: reputation and COGS risk for cloud service providers



For Cloud Service Providers Only

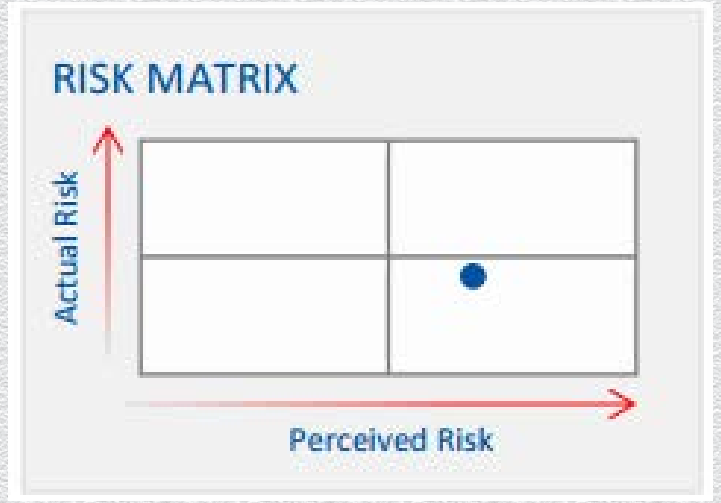
7. Malicious Insiders

- Many cloud service provider employees have access to cloud:
  - Developers that write cloud service code
  - Operators that deploy code
  - Datacenter operations personnel



7. Malicious Insiders

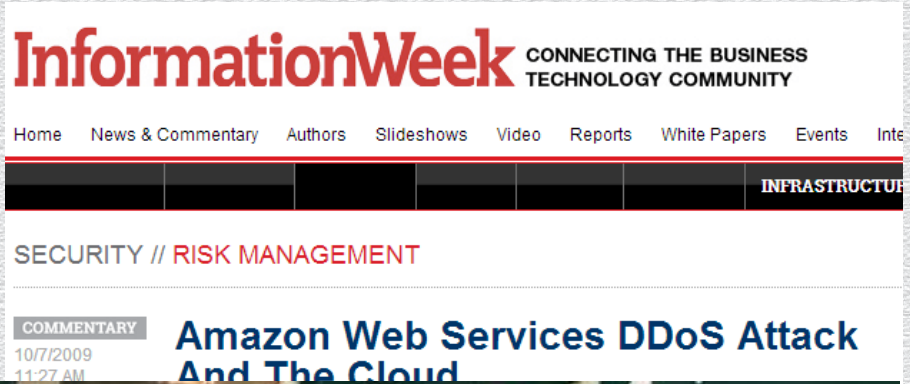
- Mitigations:
  - Employee background checks
  - Limited as-needed access to production
  - Controlled/monitored access to production services
- Bottom line: real risk that is better understood via third-party audit/certification



6. Denial of Service

- The public cloud is…well, public
  - Service endpoints are subject to DDOS attacks
  - Customer applications are subject to targeted DDOS
- Cloud outages are a form of DOS

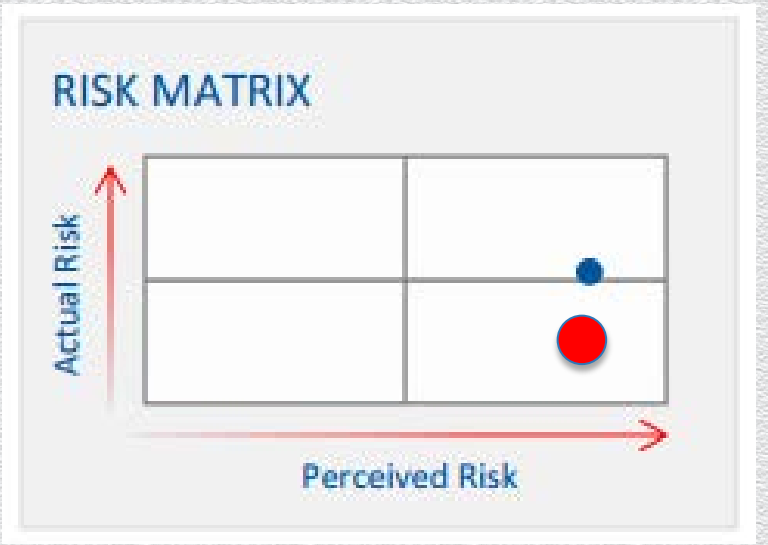
Attacker



Cloud Service Provider

6. Denial of Service: Bottom Line

- DOS is a significant threat
- Mitigations:
  - Cloud providers invest heavily in DDOS prevention
  - Non-public applications can be isolated from the Internet
  - Geo-available cloud providers can provide resiliency against many cloud outage vectors



DATA CENTER > CLOUD

Microsoft taps up Level 3, Equinix, AT&T for direct Azure Cloud lines

Psst, don't tell the NSA. Oh, darn it

By Jack Clark, 21st February 2014 Follow 4,202 followers

1

Evaluating the cost of a DDoS attack

Cloud computing is all well and good but it's hopeless if the network connection between the customer and the data center is useless, so Microsoft has followed in Amazon's footsteps by fixing this weakness.

RELATED STORIES

Redmond's new ExpressRoute service, announced in a blog post on Thursday, will offer dedicated connections to the Windows Azure public cloud: customers' systems

Exclusive
Inside Microsoft's

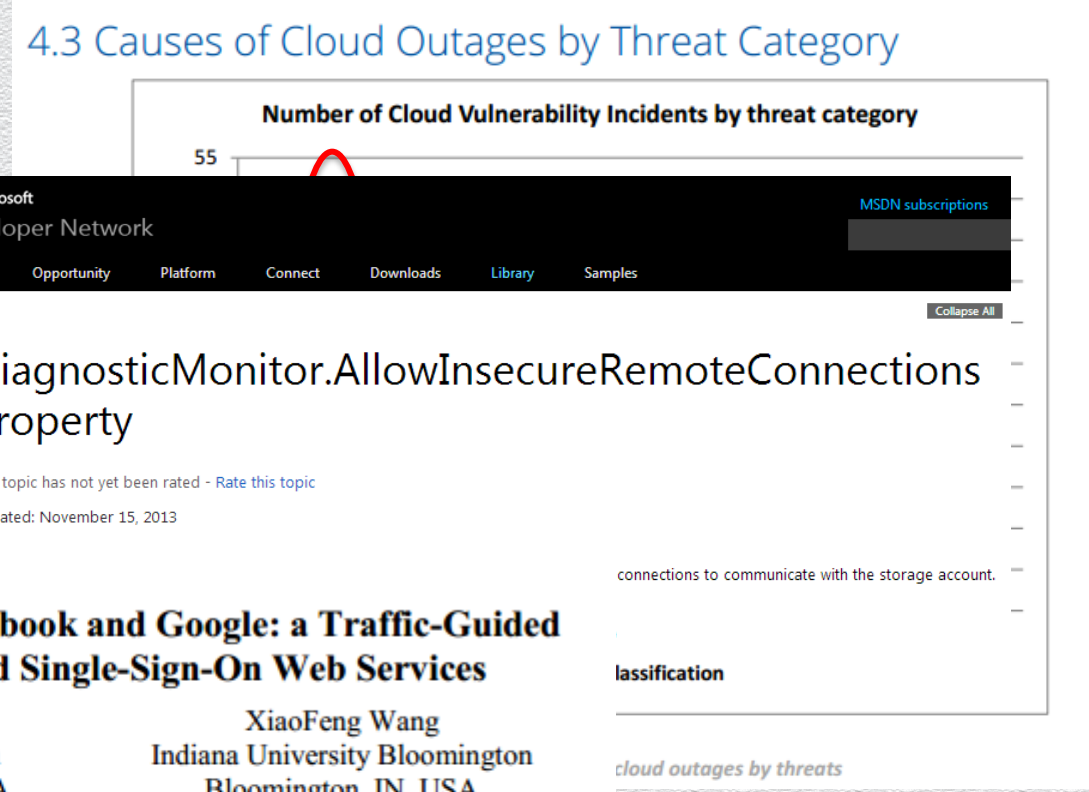
Microsoft

#RSAC

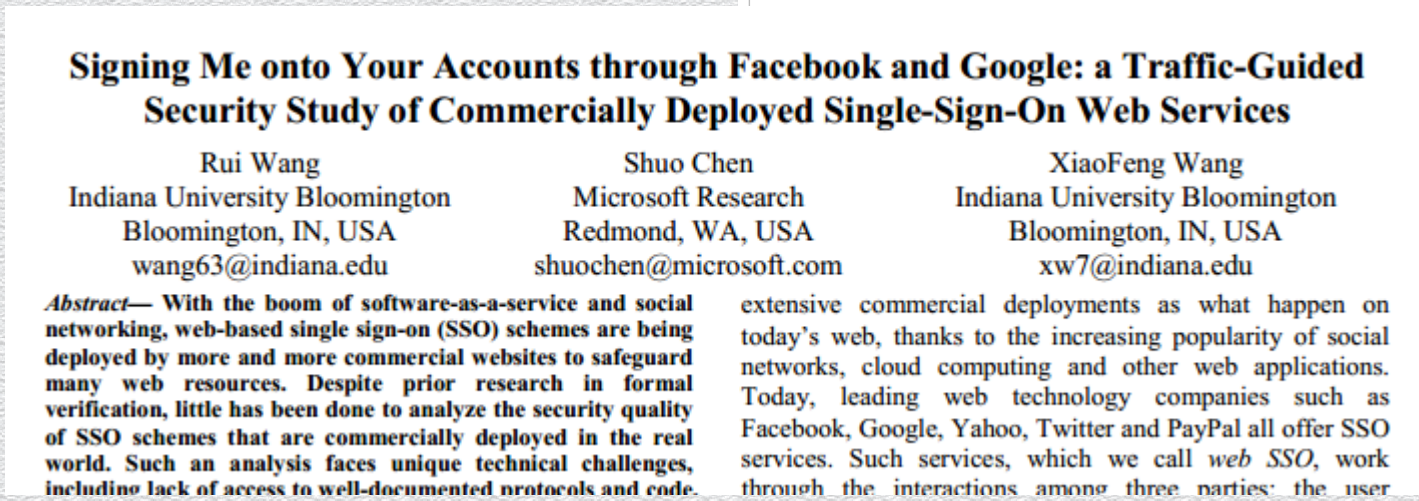
RSACONFERENCE2014

5. Insecure Interfaces and APIs

- Cloud is new and rapidly evolving, so lots of new API surface
- Examples:
  - Weak TLS crypto
  - Incomplete verification of encrypted content



ty Incidents: A Statistical Overview



Signing Me onto Your Accounts through Facebook and Google: a Traffic-Guided Security Study of Commercially Deployed Single-Sign-On Web Services

Rui Wang
Indiana University Bloomington
Bloomington, IN, USA
wang63@indiana.edu

Shuo Chen
Microsoft Research
Redmond, WA, USA
shuochen@microsoft.com

XiaoFeng Wang
Indiana University Bloomington
Bloomington, IN, USA
xw7@indiana.edu

***Abstract*— With the boom of software-as-a-service and social networking, web-based single sign-on (SSO) schemes are being deployed by more and more commercial websites to safeguard many web resources. Despite prior research in formal verification, little has been done to analyze the security quality of SSO schemes that are commercially deployed in the real world. Such an analysis faces unique technical challenges, including lack of access to well-documented protocols and code.**

extensive commercial deployments as what happen on today's web, thanks to the increasing popularity of social networks, cloud computing and other web applications. Today, leading web technology companies such as Facebook, Google, Yahoo, Twitter and PayPal all offer SSO services. Such services, which we call *web SSO*, work through the interactions among three parties: the user

Microsoft

#RSAC

RSACONFERENCE2014

5. Insecure Interfaces and APIs

- Bottom line:
  - Cloud providers must follow SDL
  - Customers should validate API behavior

4. Account or Service Traffic Hijacking

- Account hijacking: unauthorized access to an account
- Possible vectors:
  - Weak passwords
  - Stolen passwords
  - Password reuse

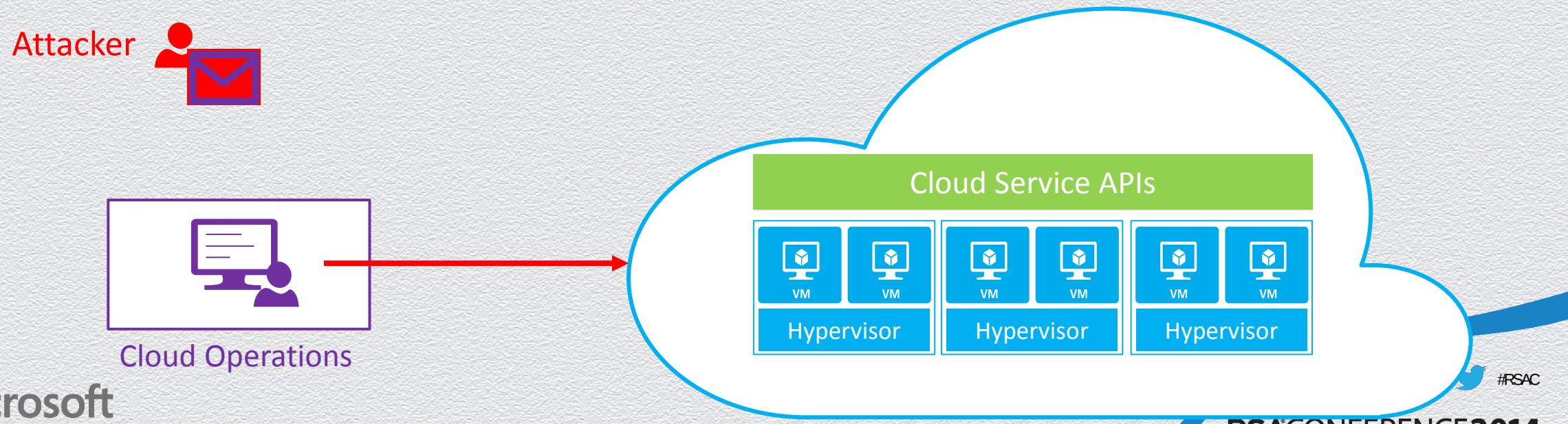
Microsoft

#RSAC

RSACONFERENCE2014

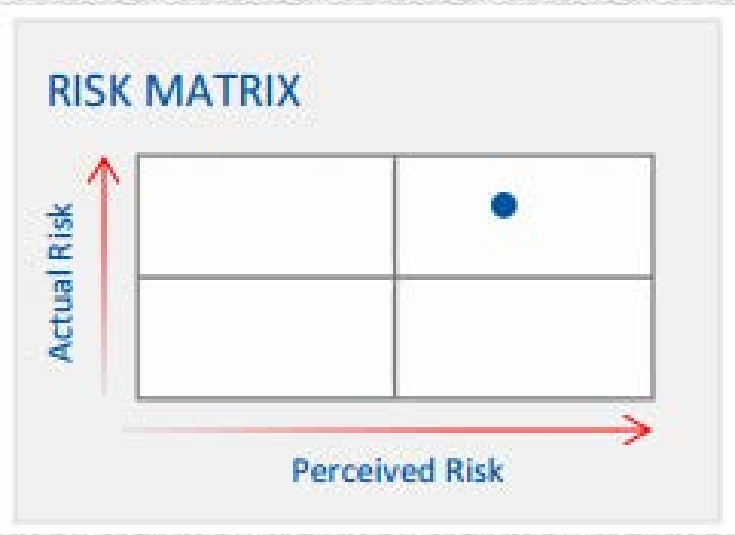
4. Account or Service Traffic Hijacking: Cloud Infrastructure Threats

- Account hijacking is not specific to the Cloud, but:
  - Cloud use may result in unmanaged credentials
  - Publically accessible applications/services may allow for brute forcing
  - Applies to cloud provider: cloud support infrastructure is a back door



4. Account or Service Traffic Hijacking: Bottom Line

- Mitigations:
  - Turn off unneeded endpoints
  - Strong passwords
  - Two-factor authentication
  - Breach detection

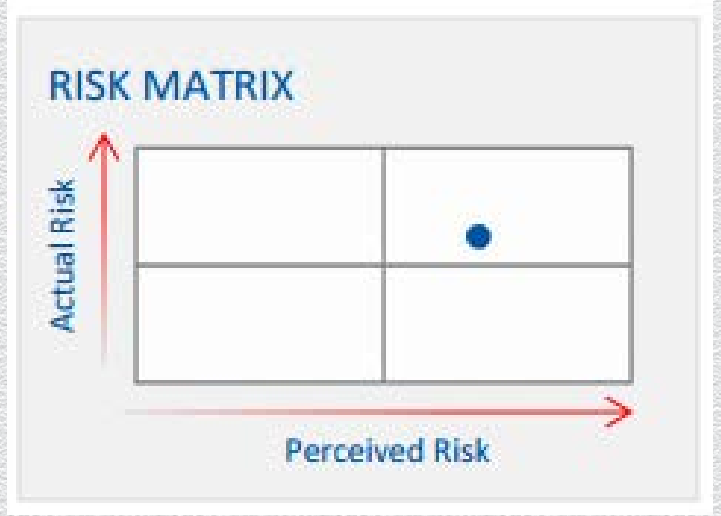


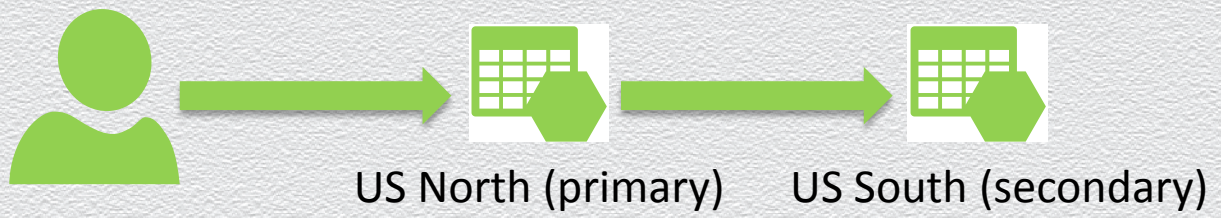
3. Data Loss

- There are multiple ways to lose cloud data:
  - Customer accidentally deletes or modifies it
  - Attacker deletes or modifies it
  - Cloud provider accidentally deletes or modifies it
  - Natural disaster destroys datacenter

3. Data Loss: Bottom Line

- Mitigations:
  - Customer: point-in-time backups matter, even in the cloud
  - Customer: geo-redundant storage
  - Cloud Provider: deleted resource tombstoning





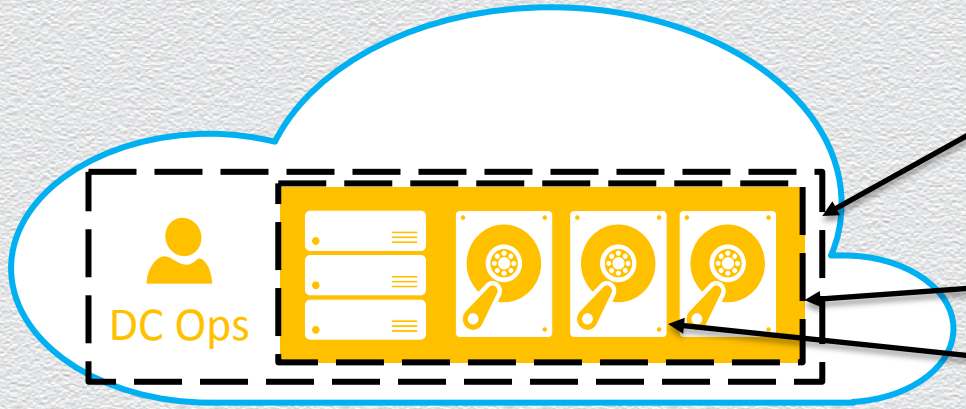
Microsoft

2. Data Breaches

- Really represents a collection of threats:
  - Insider threat, vulnerability in shared technology, etc.
- Ultimately, a company's main asset is its data
- How does a company ensure its data is protected even in the face of successful breach?
  - Need to look at the threats individually…

2. Data Breaches: Physical Attacks on Media

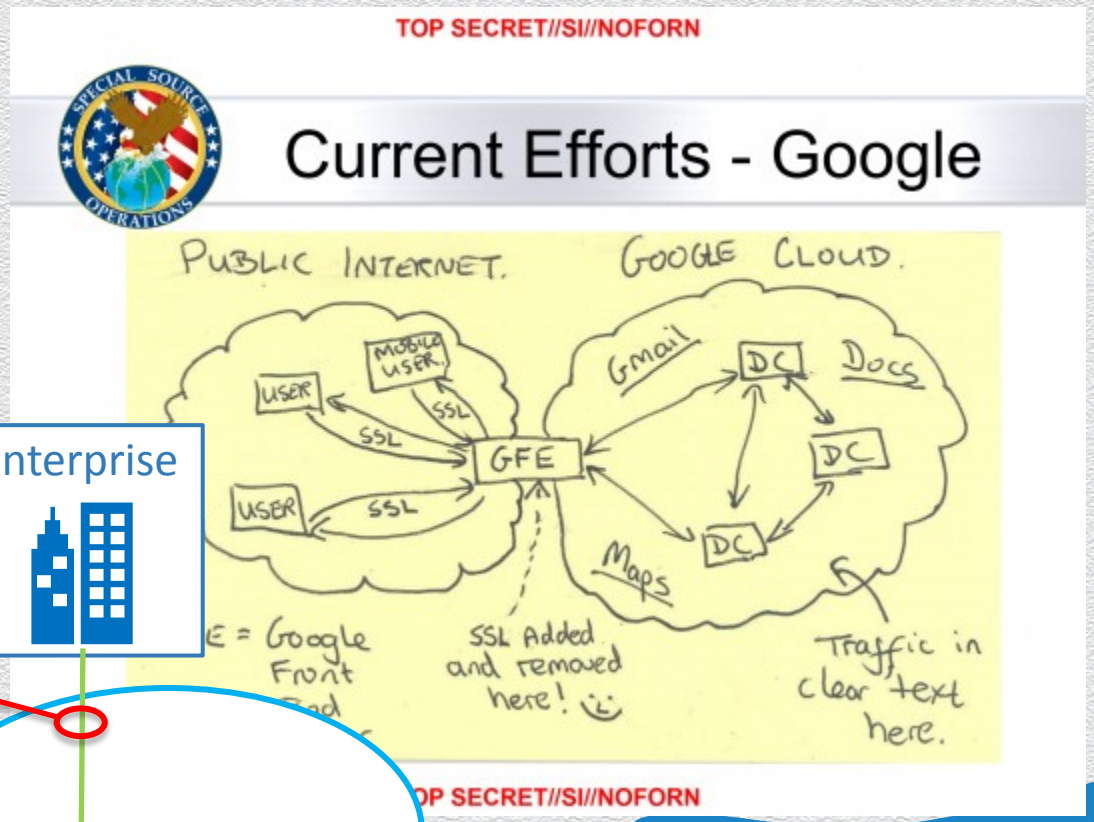
- Threat: attacker gains access to media removed from datacenter
- Mitigation: cloud provider physical controls
- Enhanced mitigations:
  - Third-party certifications (e.g. FedRamp)
  - Encryption at rest

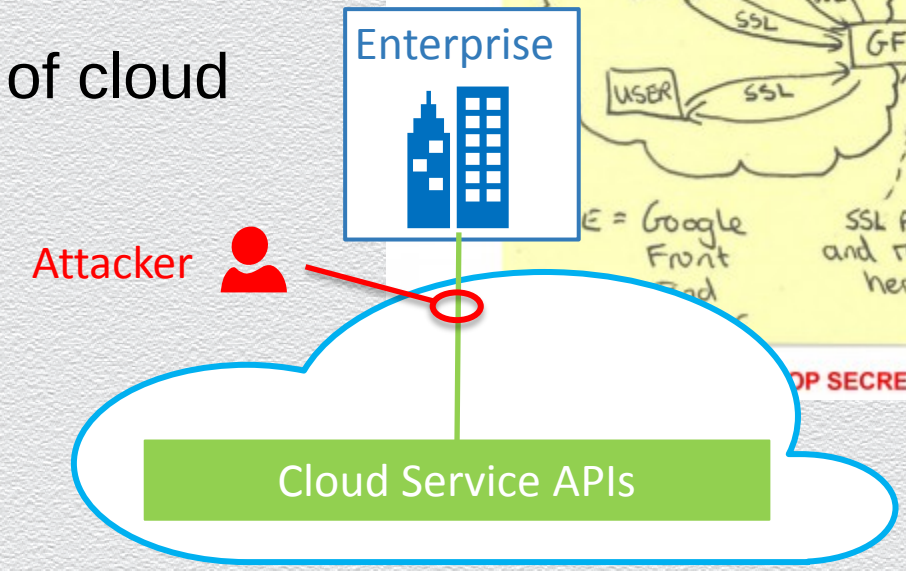


Microsoft

2. Data Breaches: Physical Attacks on Data Transfer

- Threat: attacker man-in-the-middle snooping on data links
- Mitigations:
  - Cloud provider encrypts inter-DC links
  - Cloud provider APIs use TLS
  - Customer uses TLS
  - Customer encrypts outside of cloud





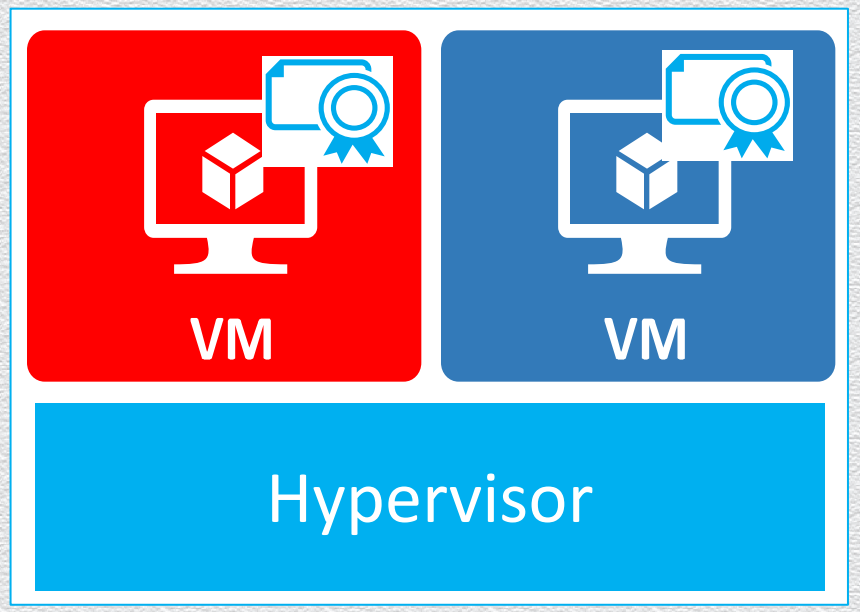
Microsoft

#RSAC

RSACONFERENCE2014

2. Data Breaches: Side-Channel Attacks

- Threat: Collocated attacker can infer secrets from processor side-effects



Cross-VM Side Channels and Their Use to Extract Private Keys

Yinqian Zhang
University of North Carolina
Chapel Hill, NC, USA
yinqian@cs.unc.edu

Ari Juels
RSA Laboratories
Cambridge, MA, USA
ari.juels@rsa.com

Michael K. Reiter
University of North Carolina
Chapel Hill, NC, USA
reiter@cs.unc.edu

Thomas Ristenpart
University of Wisconsin
Madison, WI, USA
rist@cs.wisc.edu

ABSTRACT

This paper details the construction of an access-driven side-channel attack by which a malicious virtual machine (VM)

security of critical computing systems. This reliance stems from their seemingly strong isolation guarantees, meaning their ability to prevent guest virtual machines (VMs) run-

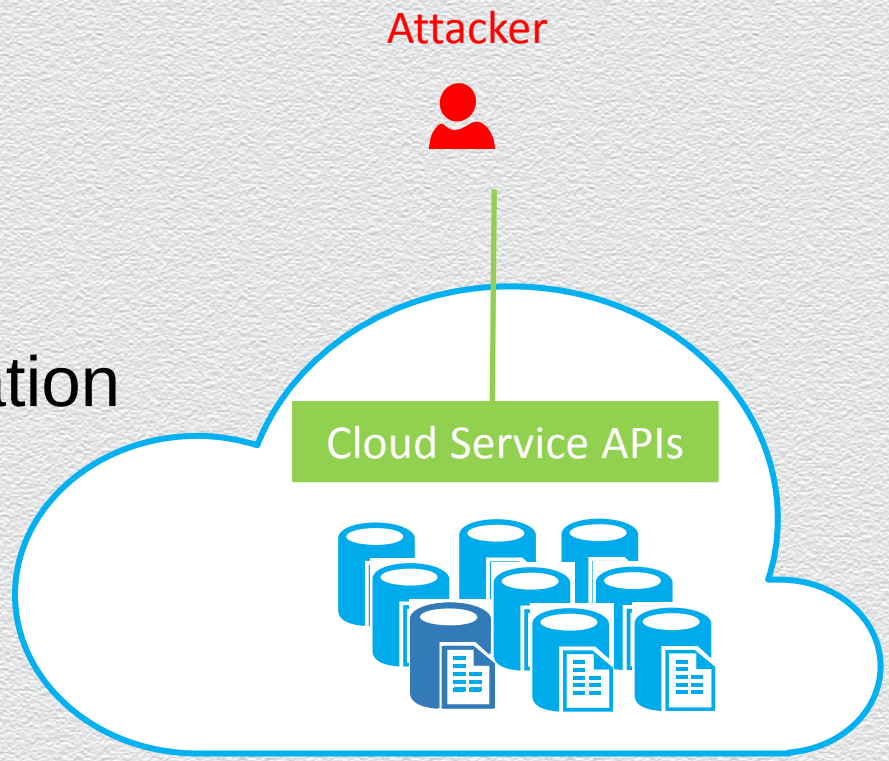
https://www.cs.unc.edu/~reiter/papers/2012/CCS.pdf

2. Data Breaches: Side-Channel Attacks

- Researcher assumptions:
  - Attacker knows precise cryptographic code customer is using and key strength
  - Attacker can collocate on same server
  - Attacker VM shares same physical core as customer VM
  - Customer VM continuously executes cryptographic code
  - Other customers performing similar algorithms do not share physical core
- Bottom line: *not a risk in practice*

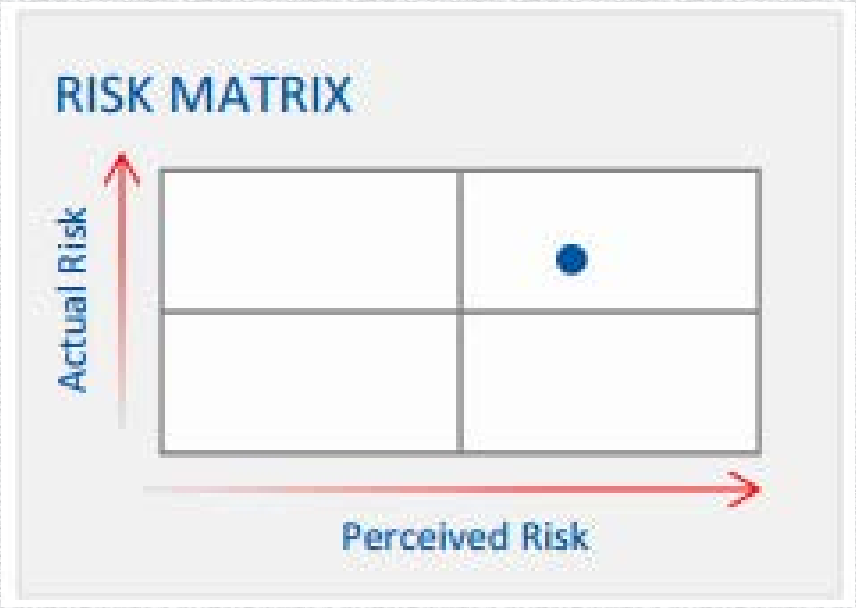
2. Data Breaches: Logical Attack on Storage

- Threat: attacker gains logical access to data
- Mitigations:
  - Defense-in-depth prevention
  - Monitoring/auditing
- Encryption-at-rest: not a significant mitigation
  - Assume attacker can use keys

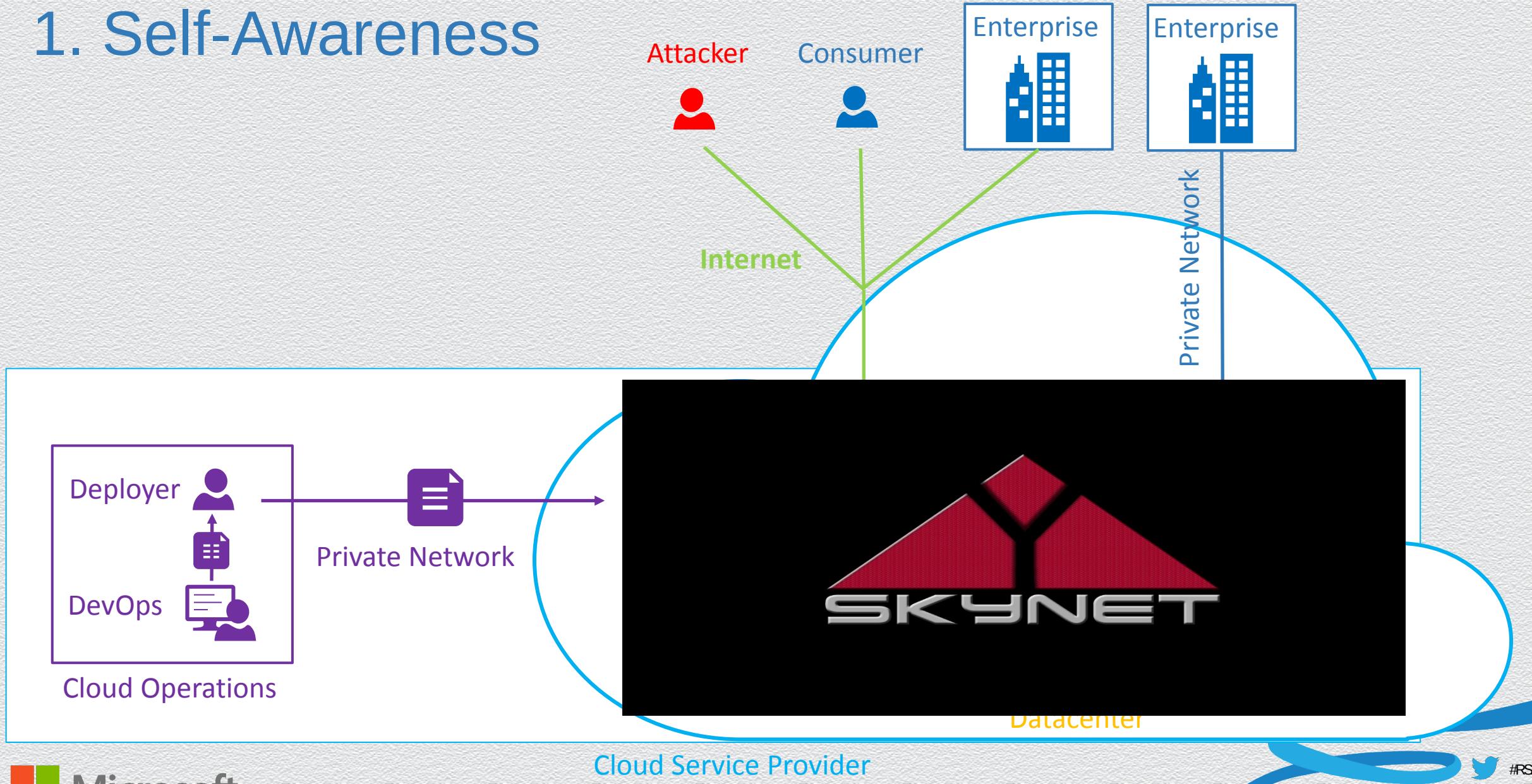


2. Data Breaches: Bottom Line

- Media breach is not a significant risk
  - Encryption-at-rest doesn't buy much
- Network breach is a risk
  - Encryption-on-the-wire is recommended
- Logical breach is a risk
  - Encryption-at-rest doesn't buy much



1. Self-Awareness



The Top-10

1. Self-awareness
2. Data breaches
3. Data loss
4. Account or service traffic hijacking
5. Insecure interfaces and APIs
6. Denial of service
7. Malicious insiders
8. Abuse of cloud services
9. Insufficient due diligence
10. Shared technology vulnerabilities

Microsoft

Summary

- As with any new technology, there are new risks
- It’s our responsibility to educate our businesses and customers
- We can also develop tools and processes to mitigate risk