# Cloud Computing Security

Myths and Realities

By

Gideon J. Lenkey CISSP

The Gold Standard in Network Security

RaSecurity.com

# Shameless Plug

- Co-Founder of Ra Security Systems, Inc.
- Managed Security Services and Security Assessments
- Buy my book: Gray Hat Hacking 3rd ed.
- See me in a movie: Code 2600
- “Google” me or grab a brochure

The Gold Standard
in Network
Security

RaSecurity.com

# What We’ll Cover

- The Cloud Security Paradigm
- Clouds side risks
- Threats from your end
- Everything in the middle
- Recommendations

The Gold Standard
in Network
Security

RaSecurity.com

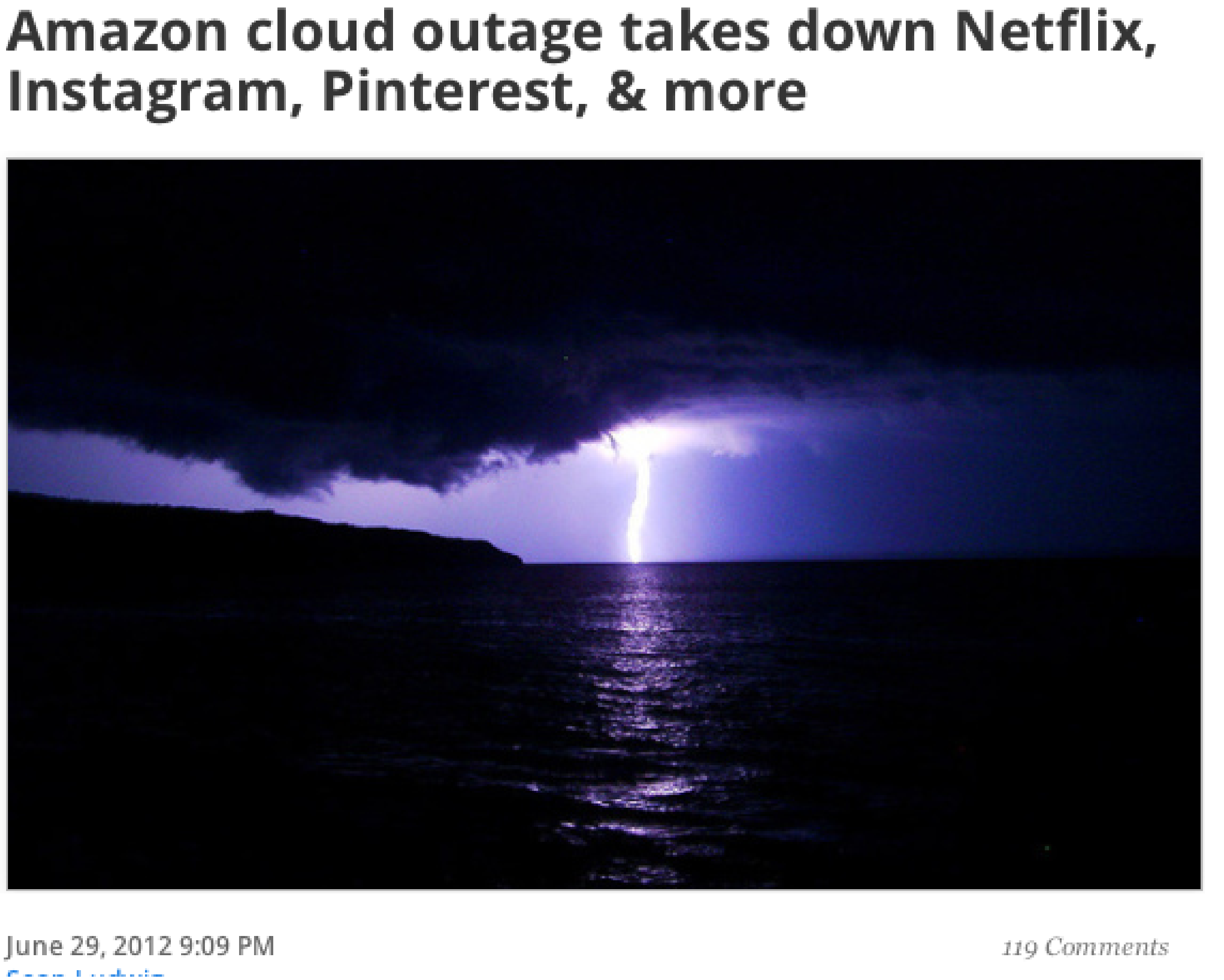
# The Cloud Security Paradigm

- Better managed
- More fault tolerant
- Cheaper
- Pay as you go

The Gold Standard
in Network
Security

RaSecurity.com

# What could possibly go wrong?



## Amazon cloud outage takes down Netflix, Instagram, Pinterest, & more

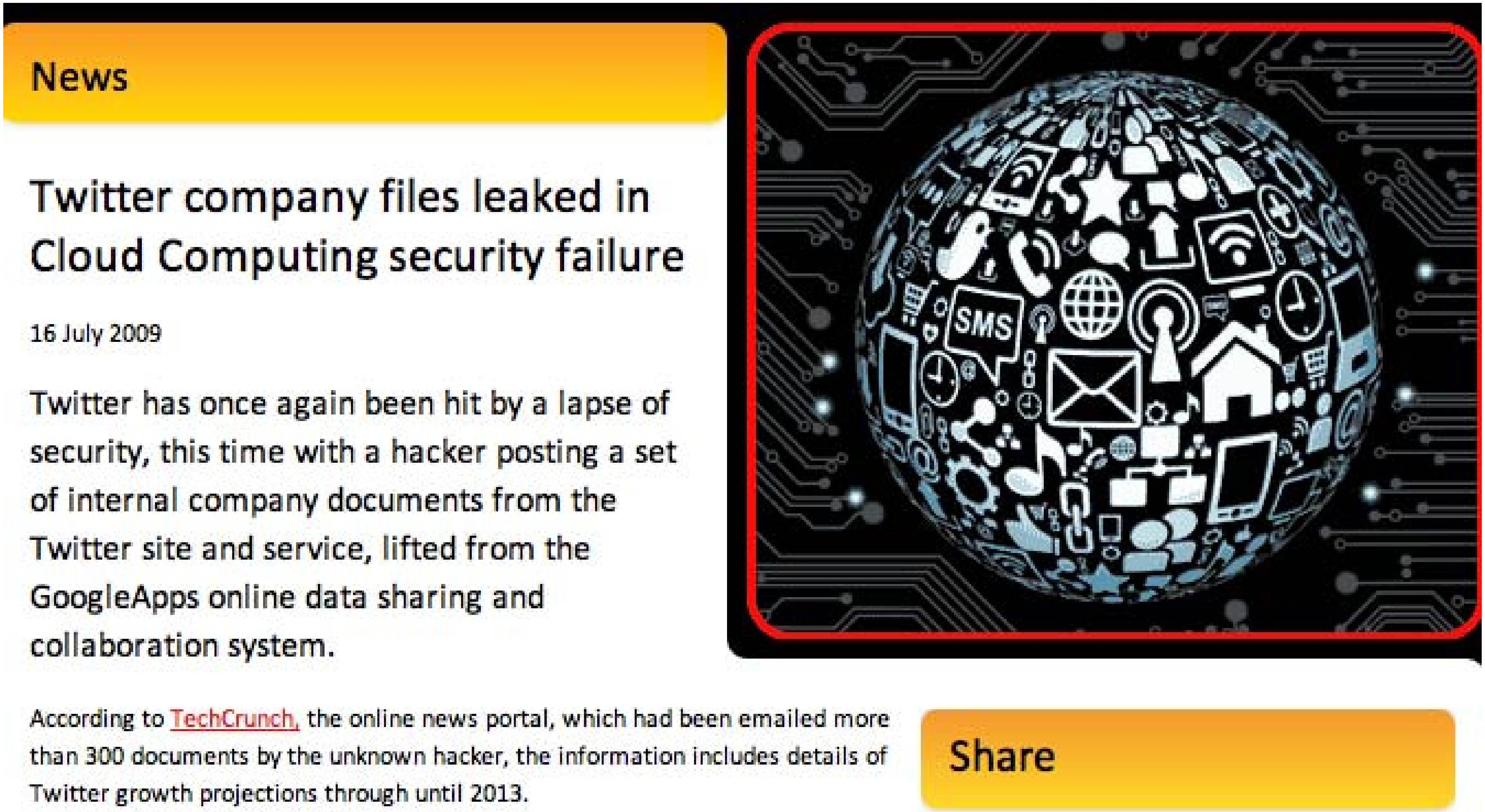
June 29, 2012 9:09 PM

*119 Comments*

The Gold Standard in Network Security

RaSecurity.com

# Let’s not forget the human factor



News

## Twitter company files leaked in Cloud Computing security failure

16 July 2009

Twitter has once again been hit by a lapse of security, this time with a hacker posting a set of internal company documents from the Twitter site and service, lifted from the GoogleApps online data sharing and collaboration system.

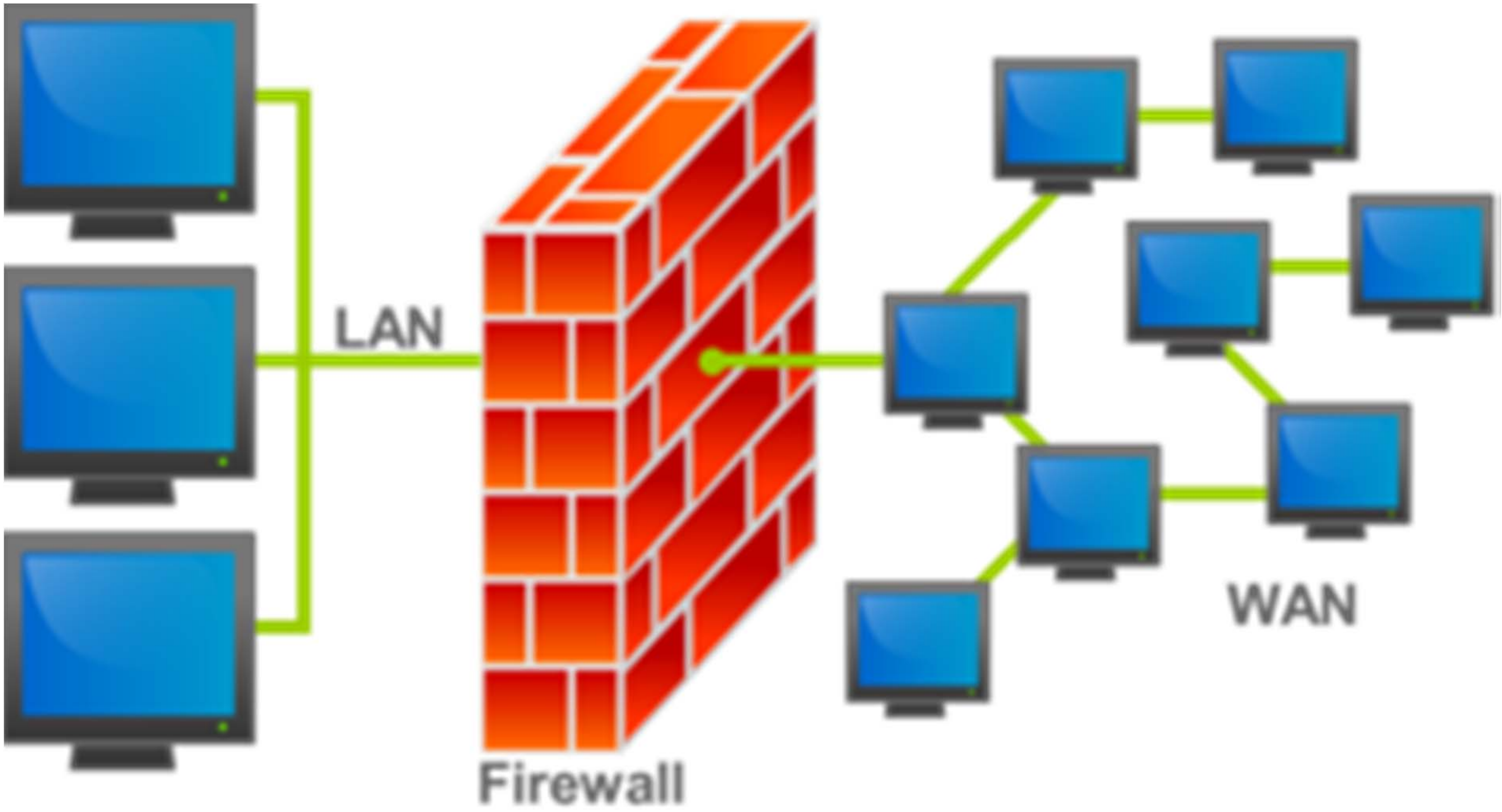
According to TechCrunch, the online news portal, which had been emailed more than 300 documents by the unknown hacker, the information includes details of Twitter growth projections through until 2013.

Share

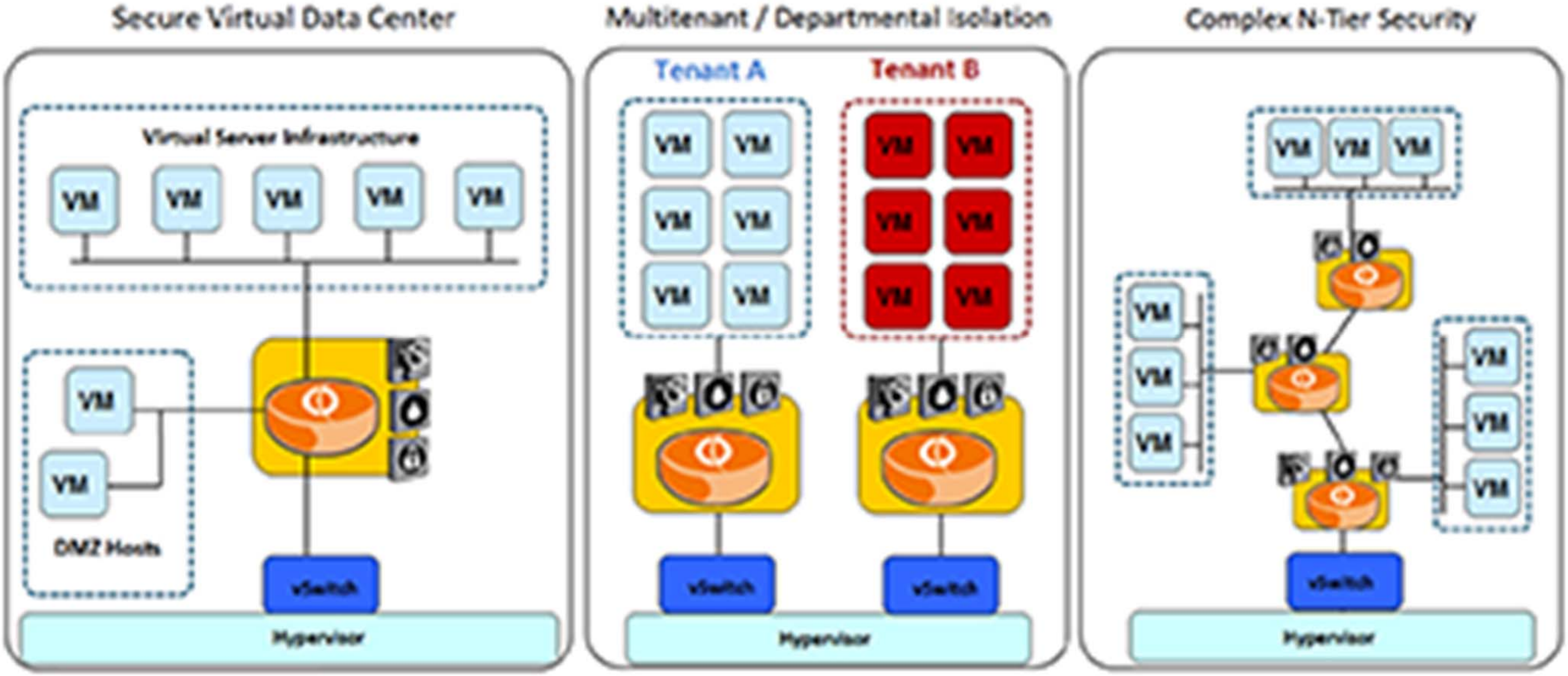
# Cloud Side Measures

- Firewall (most have)
- Server AVS (most offer)
- IDS/IPS/NSM? (few offer)
- Hardened Configuration? (ymmv)

# Traditional Firewall



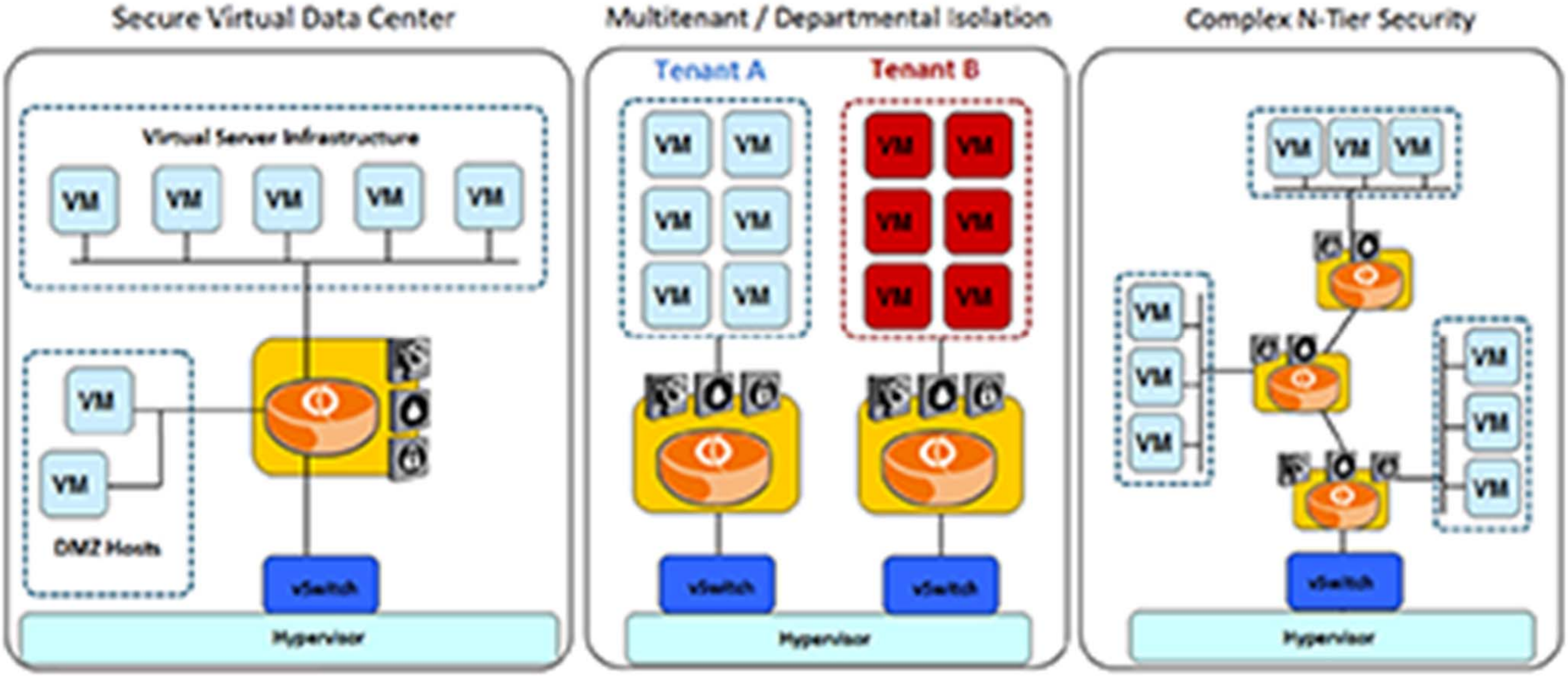
# Virtual Firewall



# Common Criticisms

- You have no idea where your data is
- You have no idea who actually has access to it
- What’s your recourse if it fails?
- What if your provider shuts you off?

# Common Threats

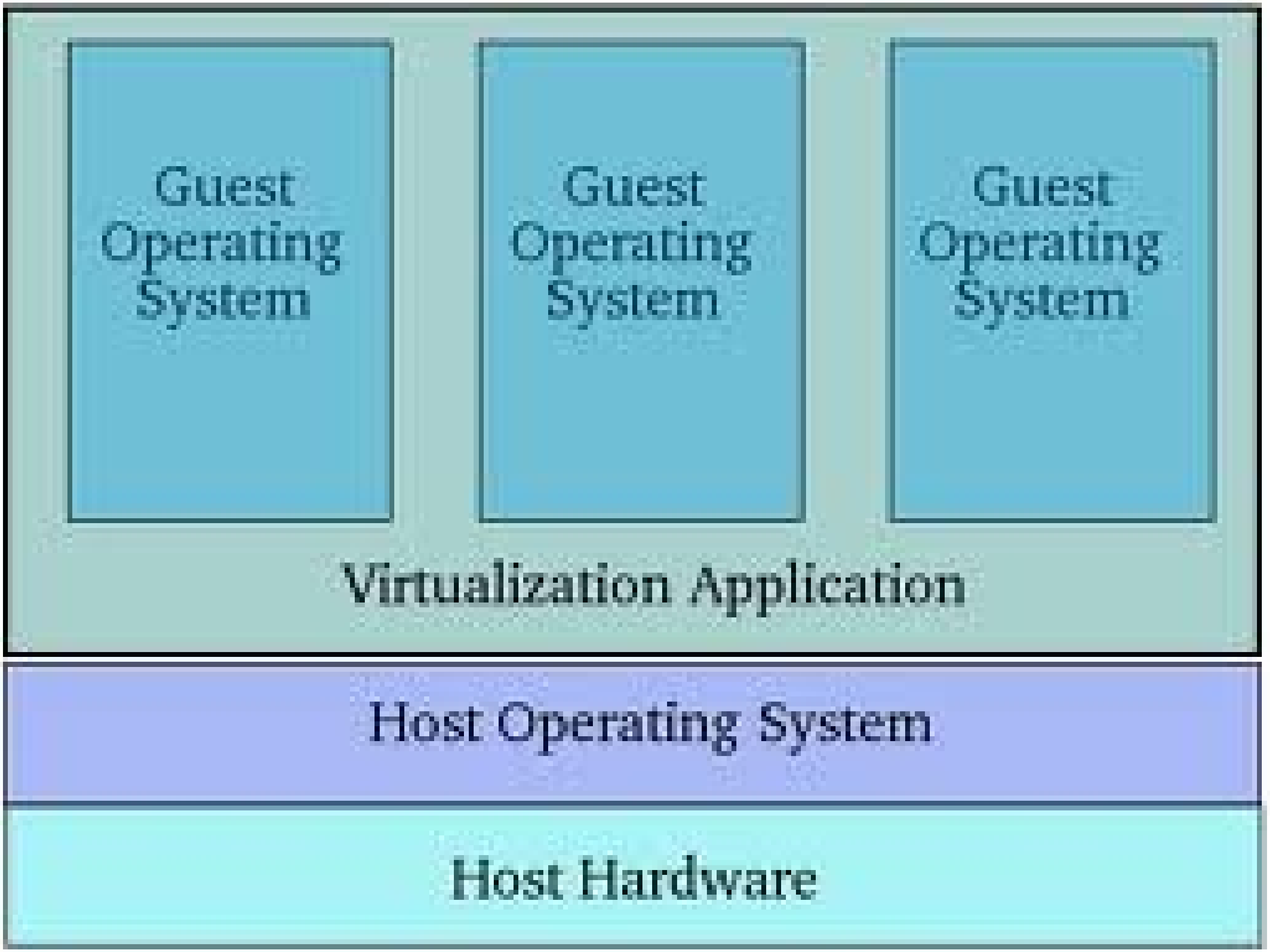


The Gold Standard in Network Security

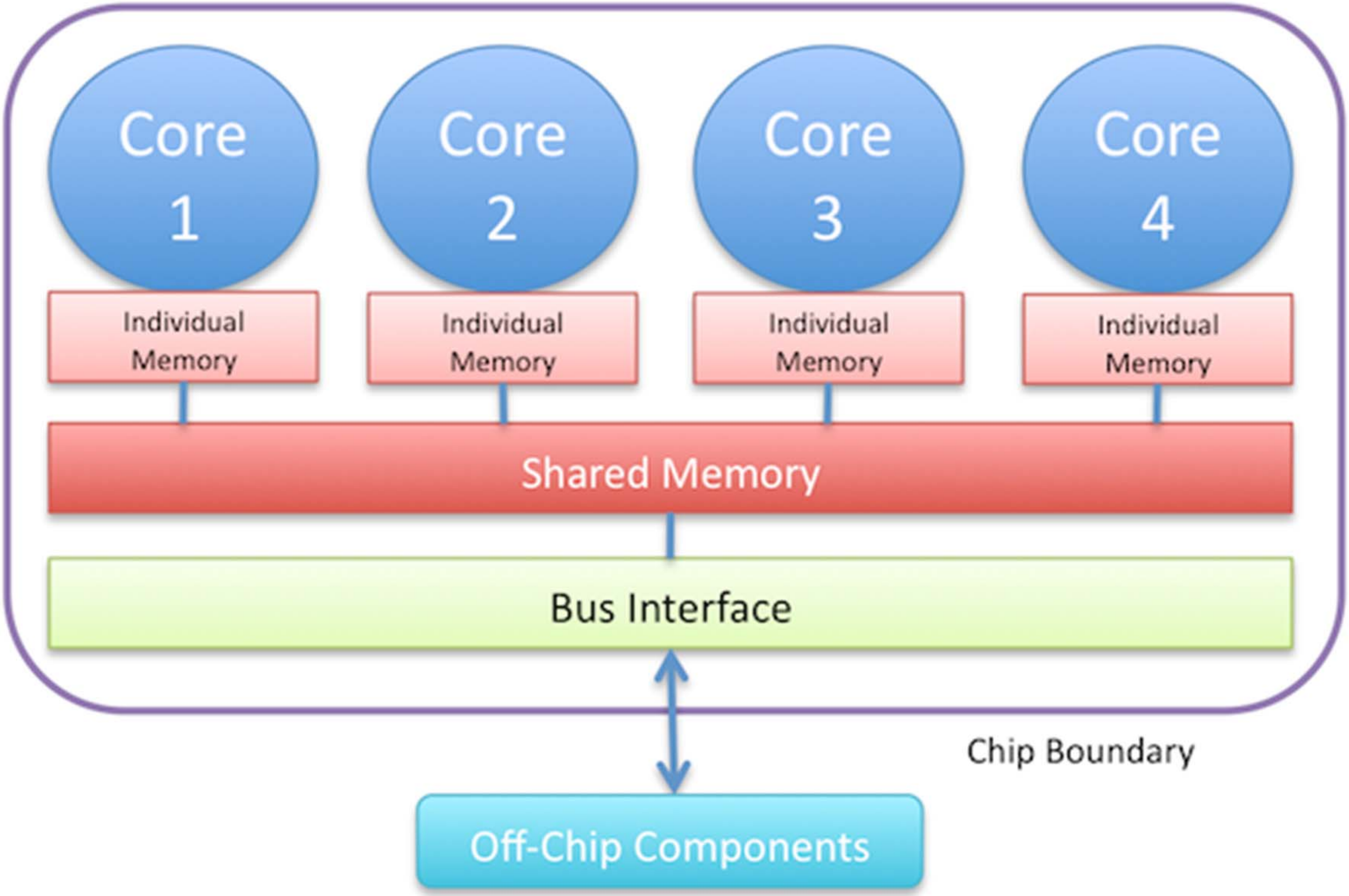
RaSecurity.com

# Un-Common Threats

- VM isolation considered a key security benefit
- Side Channel attack long theorized
- Researchers proved it in Nov 2012 paper
- Recovered a large private key from adjacent VM
- Attacker does not need to break in


Guest Operating System
Guest Operating System
Guest Operating System
Virtualization Application
Host Operating System
Host Hardware

# Multi-core Processor



Core 1

Core 2

Core 3

Core 4

Individual Memory

Individual Memory

Individual Memory

Individual Memory

Shared Memory

Bus Interface

Chip Boundary

Off-Chip Components

# Side Channel Attack

“So the bottom line remains: Co-residency is not safe for highly sensitive workloads.”

--Ari Juels, chief scientist at EMC's RSA security division

The Gold Standard in Network Security

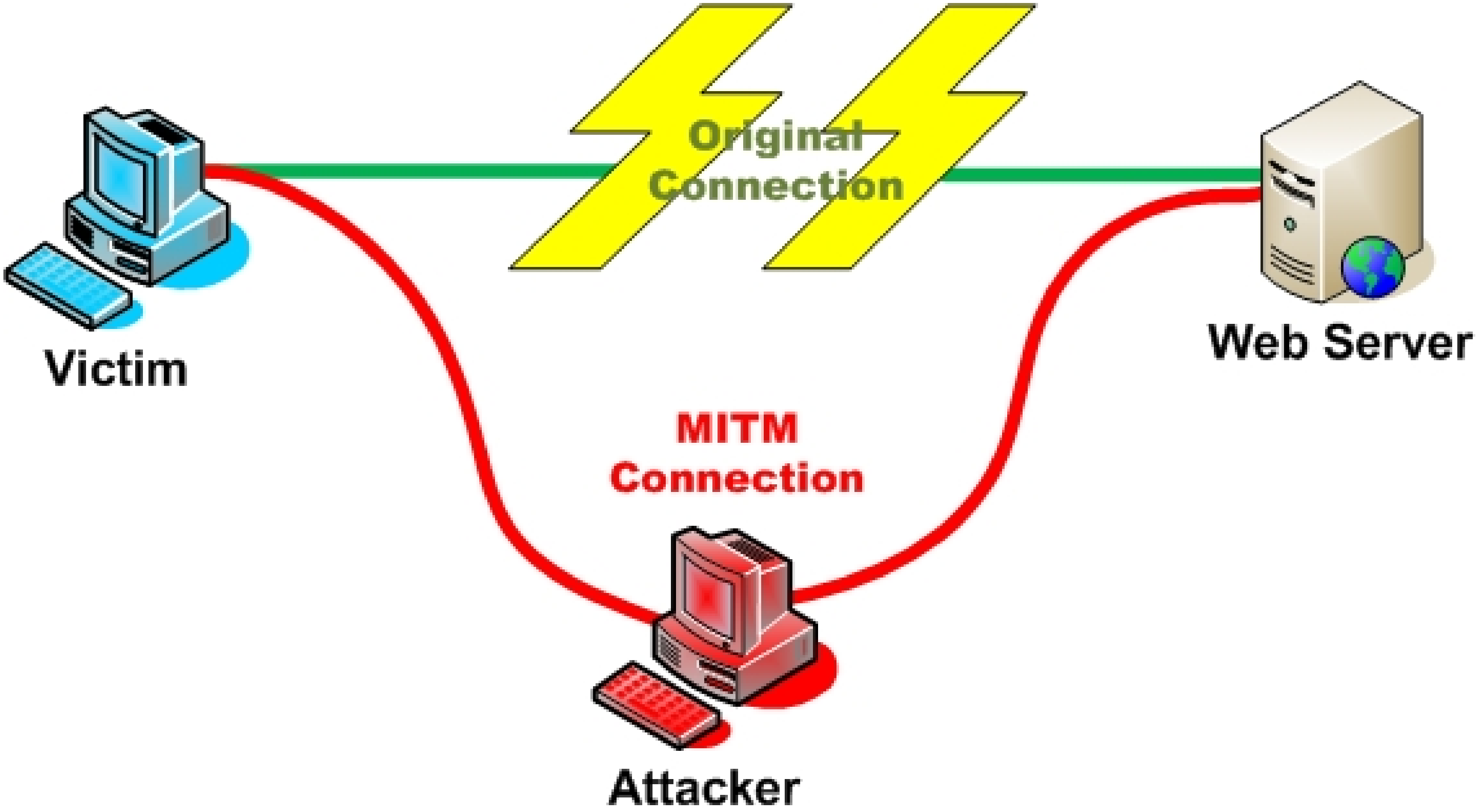
RaSecurity.com

# Man in the Middle Attacks

- Username and password
- Fake Login Screens
- Session Data
- Traffic Analysis
- Traffic Redirection
- Remote Exploit Injection

The Gold Standard
in Network
Security

RaSecurity.com


Original Connection
Victim
Web Server
MITM Connection
Attacker

# Client Side Attack

- Same as any other infrastructure design
- Impersonation means access
- Attacker can pivot on compromised workstation
- Contemporary Malware will probably not be detected by AVS
- Malware is good at staying hidden

# Modern Malware Will

- Collect your credentials
- Search your memory and hard drive for:
    - Credentials
    - Financial Information
    - Session Data
- Leaves a way back in
- Can even watch and listen to you

# What Can I Do?

- Understand what the responsibilities of the provider are
- Use cloud service providers for their strengths and compensate for their weaknesses
- Keep up your security practices on the home front
- Always utilize detective controls even in the cloud environment
- Treat each VM as a SPoF
- If you have remote users, consider Two Factor Authentication

The Gold Standard
in Network
Security

RaSecurity.com

# Fin

Gideon J. Lenkey, CISSP

glenkey@rasecurity.com

(908) 246-0634

The Gold Standard in Network Security

RaSecurity.com