Cloud Security
Fortify Your Assets

MENA Information Security Conference 2011
September 18th – 19th 2011

Bashar Bashaireh
Regional Director,
Fortinet Middle East
bbashaireh@fortinet.com

1. **Introduction**
2. Cloud Computing Background
3. Challenges
4. Securing the Cloud
5. Security Consolidation
6. Q & A

Fortinet : A Real Security Label

Fortinet, Inc.

- $375 million billings in 2010; +33% YoY growth
- Consistently strong sequential growth
- Profitable: $468 million cash
- 1,500+ employees and 30+ offices
- Middle East offices in Dubai, Riyadh, Abu Dhabi and Cairo
- Shipped 750,000+ appliances to date
- 100,000+ customers and 5,000+ channel partners

Best-in Class Technology

2010 Third-Party Recognition

Market Leadership Across the Board

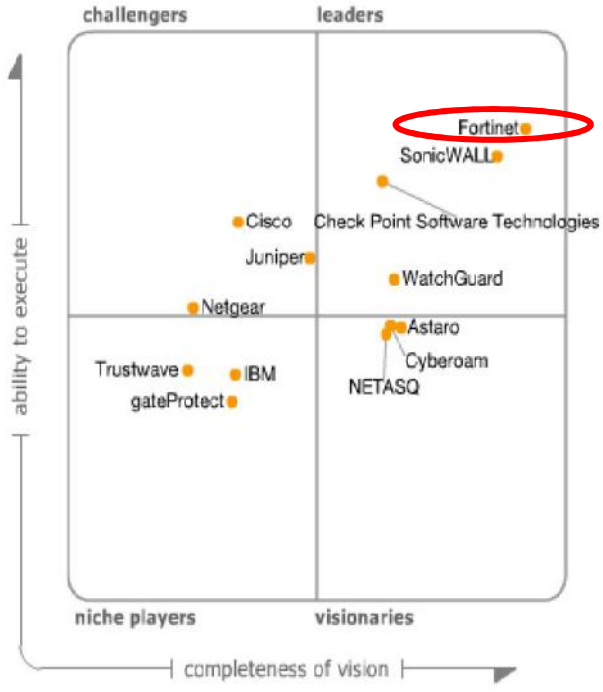
IDC *Analyze the Future*

Worldwide UTM Market Share Q4 2010 (1)

Rank	Company	Market Share (%)
1	FORTINET	16.2
2	Check Point	11.8
3	Juniper	8.4
4	Cisco	6.6
5	SonicWALL	7.8
6	McAfee	6.3
7	WatchGuard	5.2
8	Crossbeam	2.6
9	Other	35.1
	Total	**100.0**

Gartner

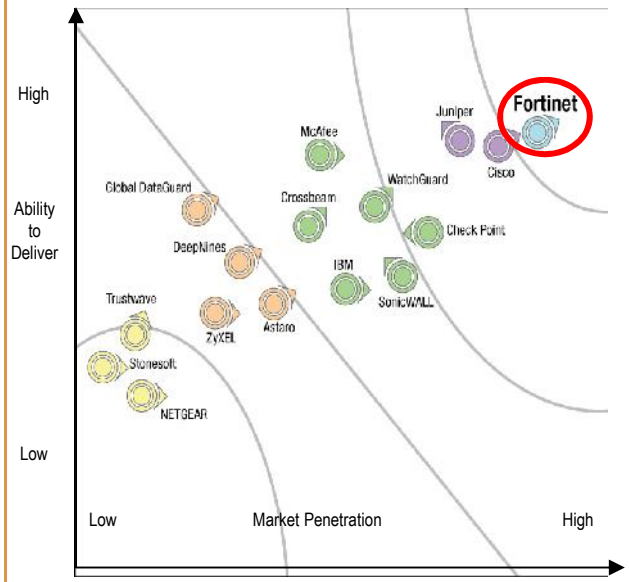
Magic Quadrant for Unified Threat Management (2)



As of October 2010

FROST & SULLIVAN

UTM Market Competitive Landscape, 2009(3)



Contender | Market Leader | Niche Participant | Specialist | Challenger

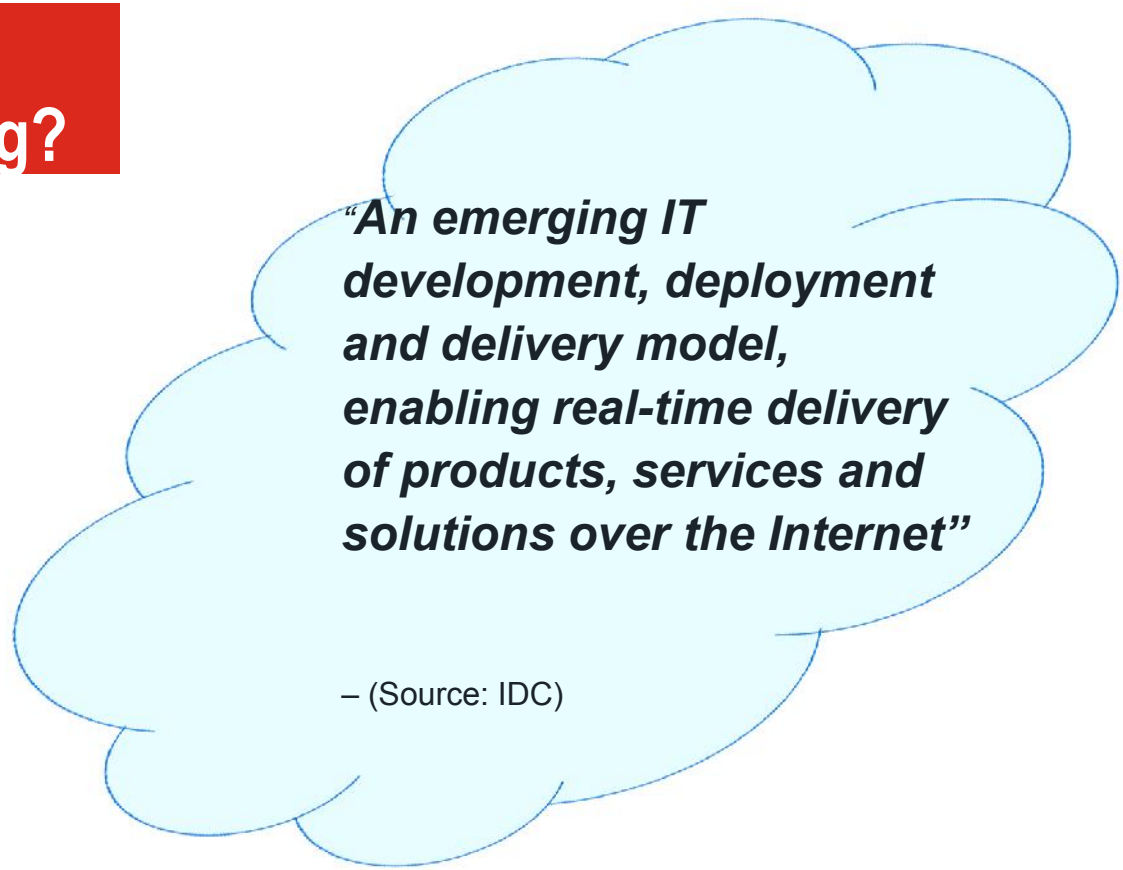
Notes

(1) IDC Worldwide Security Appliances Tracker, March 2011 (market share based on factory revenue)
(2) Gartner, "Magic Quadrant for Unified Threat Management", October 2010
(3) Frost & Sullivan, "World Unified Threat Management, Products Market 2009", 2010

1. Introduction
2. **Cloud Computing Background**
3. Challenges
4. Securing the Cloud
5. Security Consolidation
6. Q & A

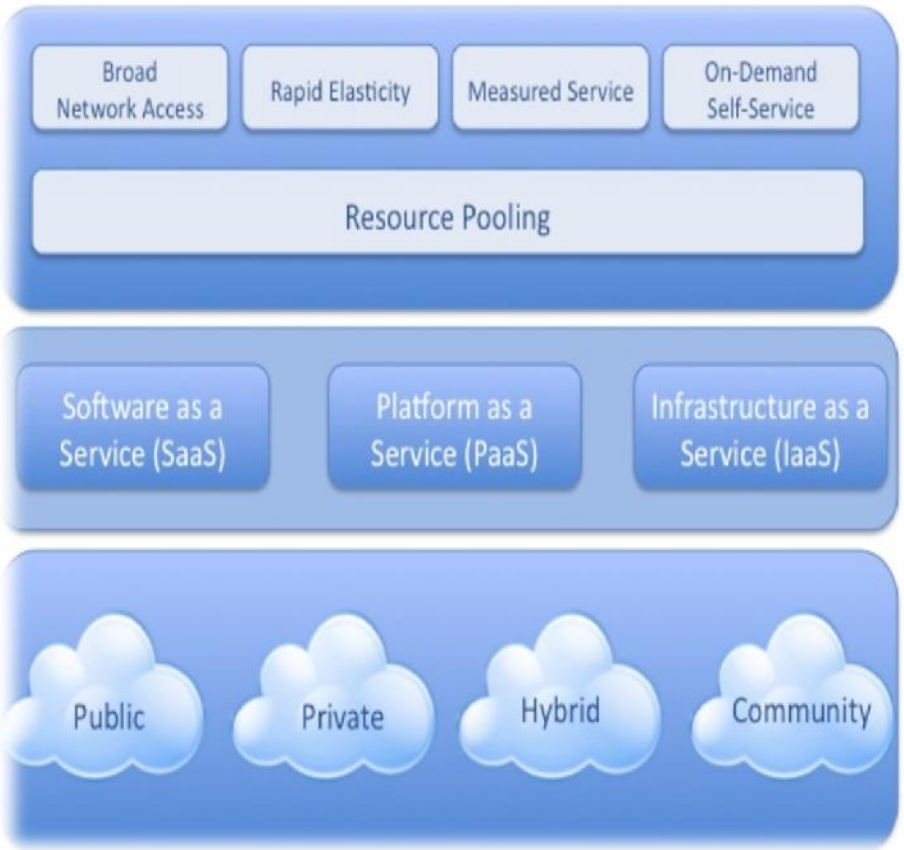
Cloud Computing Background

What is Cloud Computing?



Cloud Computing Background

NIST Visual Model of Cloud Computing Definition



Essential Characteristics

Service Models

Deployment Models

NIST defines cloud computing into

5 Essential Characteristics

3 Cloud Service Models

4 Cloud Deployment Models

Cloud Computing Background

Essential Characteristic of Cloud Computing

On-Demand Self-Service. Consumers can unilaterally provision computing capabilities as needed automatically, without human interaction with a service provider.

Broad Network Access. Network capable and can be accessed via heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).

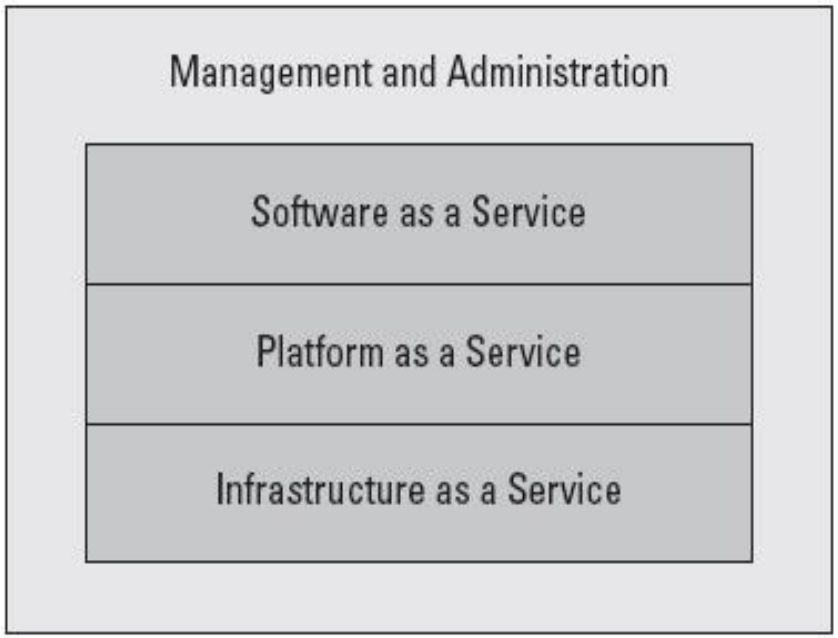
Resource Pooling. Multi-tenant model. Different physical & virtual resources dynamically assigned and reassigned according to consumer demand.

Rapid Elasticity, and ability to scale resources up and down 24x7 depending on customer demand.

Measured Service. Resources usage has to be metered for customers to be billed.

Cloud Computing Background

Cloud Service Delivery Models



- ***SOFTWARE as a SERVICE (SaaS)***
  offers purpose-built business applications.

- ***PLATFORM as a SERVICE (PaaS)***
  offers development environments (solution Stack) that IT organizations can use to create cloud-ready business applications.

- ***INFRASTRUCTURE as a SERVICE (IaaS)***
  offers computing resources that IT Orgs. use to deliver custom business solutions

All these service delivery models require proper management, administration and Security in place

Cloud Computing Background

Cloud Deployment Models

Public Cloud - A public cloud is a publically accessible cloud environment owned by a third-party cloud provider.

Community Cloud - A community cloud is similar to a public cloud except that its access is limited to a specific community of cloud consumers

Private Cloud - A private cloud is owned by a single organization.

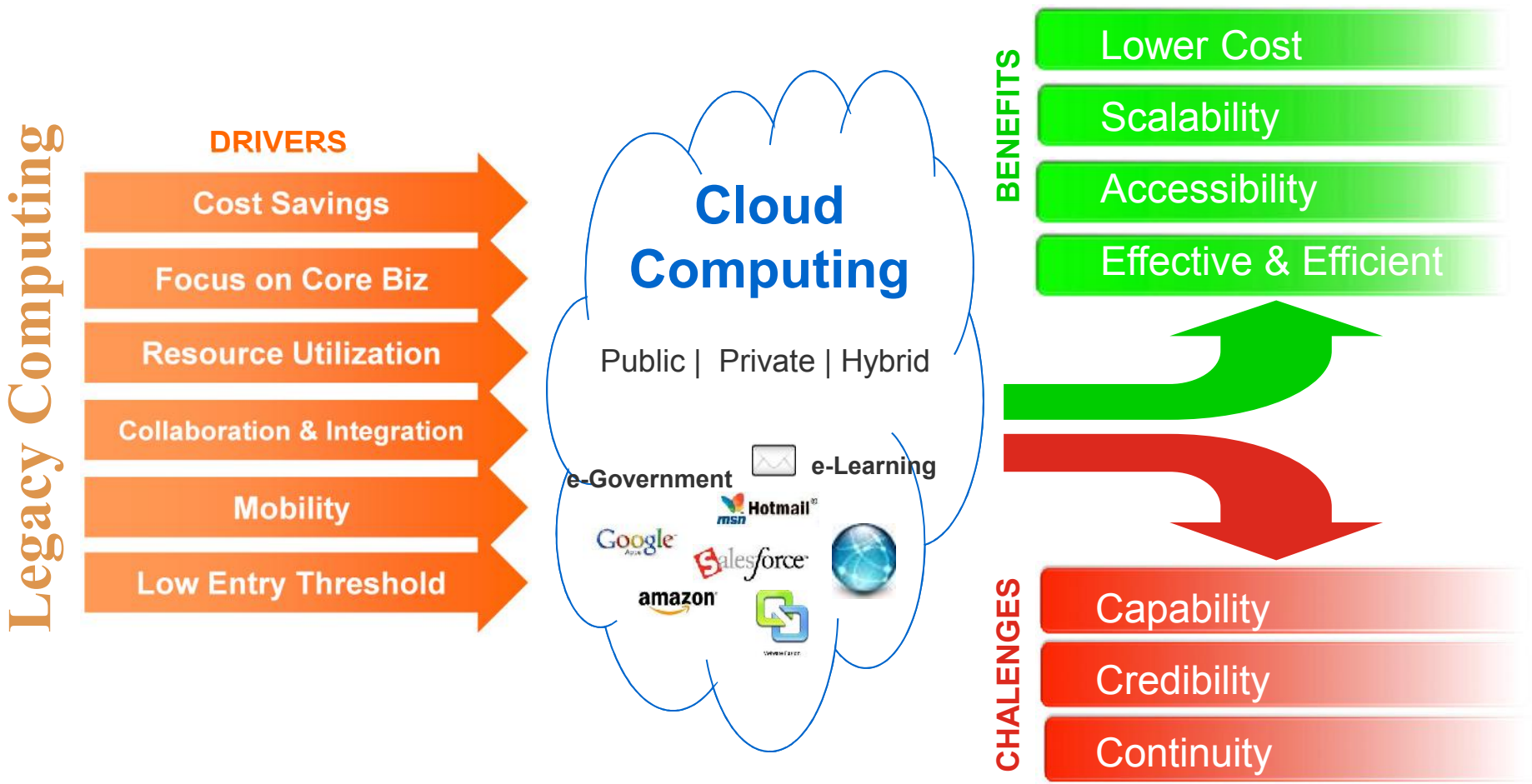
Hybrid Cloud - A hybrid cloud is a cloud environment of two or more different cloud deployment models.

Cloud Opportunity

- Spending on Cloud Technology and Services will increase 30% by 2011
- Public Cloud Services Increased 34% in 2010 to nearly $22 billion
- 13% of Small Firms and more than 30% of Midsize firms plan to add Cloud Services in the next 12 months
- Early Adopters in the Channel are MSPs, Web Developers and Network Infrastructure/Telco VARs for Cloud Hosted Solutions

Everything Channel: Dark Clouds Ahead, Why the Mid-Market Needs to Ramp Up Cloud Security, June 2011
IDC, WW & US Security Services 2011-2015 Forecast & Analysis
IDC Small & Medium-Sized Business Special Market Update, May 2011

Cloud Computing Background



1. Introduction
2. Cloud Computing Background
3. **Challenges**
4. Securing the Cloud
5. Security Consolidation Protects Assets
6. Q & A

Ten Cloud Dos and Don'ts

1- Don't Be Reactive

2- Do Consider the Cloud a Financial Issue

3- Don't Do It Alone

4- Do Think about Your Architecture

5- Don't Neglect Governance

6- Don't Forget about Business Process

7- Do Make Security the Centerpiece of Your Strategy

8- Don't Apply the Cloud to Everything

9- Don't Forget about Service Management

10- Do Start with a Pilot Project

Securing the Cloud : The 3 Critical C's

- Is my data always there?
- Can the cloud be trusted?
- Who has access to my data?
- Can I move the data out of the cloud?
- Regulations and Compliance?
- Who controls my data?
- Integrity?
- Confidentiality?
- Survivability?

- ***CAPABILITY** : IT systems and security management capability to support the business model*

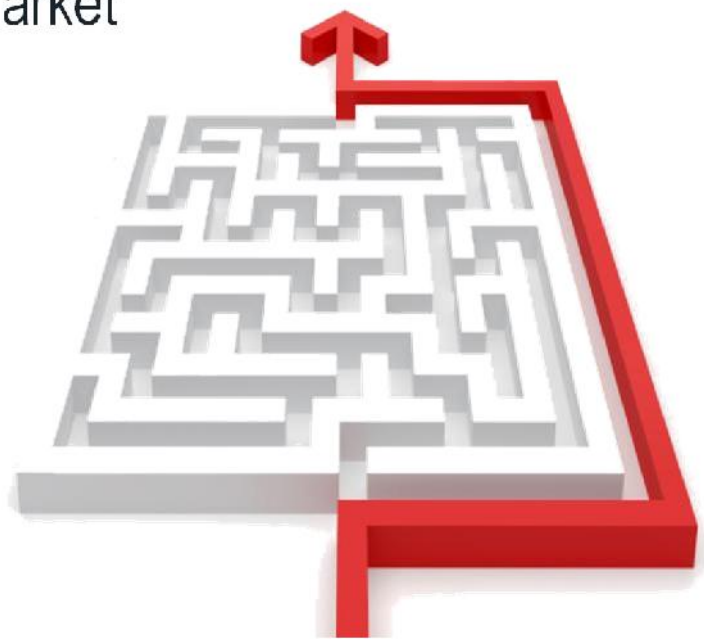
- ***CREDIBILITY** : Prove and demonstrate IT and security management effectiveness to attract customers*

- ***CONTINUITY** : Continual building of trust->brand to retain them*

1. Introduction
2. Cloud Computing Background
3. Challenges
4. **Securing the Cloud**
5. Security Consolidation
6. Q & A

Simplify Security in the Cloud for Your End Users

- Cloud Security Services Quick Time to Market
- Less Complexity
- Real Time Threat Response
- Reduce Initial Costs
- Reduce Need for Dedicated IT Staff
- Full Visibility into Network



Cloud Security Elements

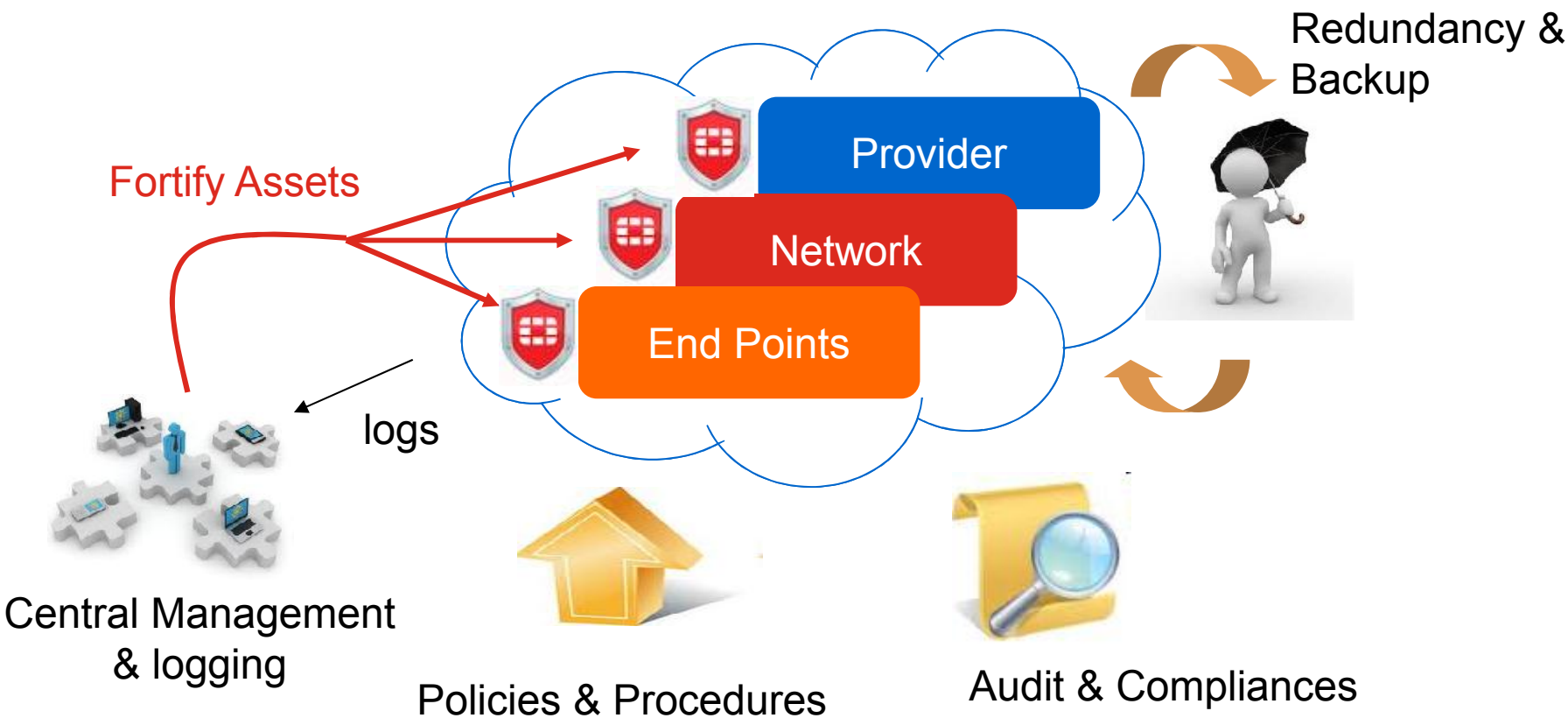
- **End Points:**
  - Physical Security
  - Anti Virus / IPS / Firewall / Email
  - VPN / Encryption

- **Cloud Infrastructure:**
  - Physical Security
  - Firewall + virtualization
  - Anti Virus / IPS
  - VPN / Encryption
  - Host security and Vulnerability Management

- **Cloud Applications & Online Information:**
  - Secure application software!
  - Authentication and access control
  - Web Application Firewall and IPS
  - Database security

- **Management & Compliancy:**
  - **Secure Policies and Processes**
  - **Compliancy and Auditing**
  - **Log Management**
  - **Backup and DR**

How to Secure the Cloud?



Fortify End Points

Physical Security

Secure all your IT assets, including PCs, Laptops, Mobile terminals against theft and physical attack.

Data Access Protection

With right credentials the cloud services are often accessible from anywhere. Protect your devices against unauthorized usage. Use authentication & encryption.

Beware of infection!

To decrease risk of unauthorized access and to protect your data from malware, trojans, key loggers and eavesdropping all attack vectors should be covered.

Physical Protection | **Access Authentication** | **Anti Virus/Spyware/ Malware**

Fortify Web based Applications

Web Application Firewall - WAF

Secures web applications to help customers meet compliance requirements

XML Firewall

Secures and prevents exploits against XML based web services

Application Acceleration

Accelerates and ensures timely delivery of web based content

Load Balancing

Assures consistent performance and availability of critical web applications

Secures Web Applications | **Protects Web Services** | **Optimises Application Delivery**

Fortify Databases

Vulnerability Assessment

Know your own vulnerabilities before everyone else does!

Activity Monitoring

See what's going on in your database, who do what and when.

Compliance

Meet industry best practices based on compliances such as HIPAA, SOX, PCI DSS

Alerting System

Get notified as soon as something wrong happened!

Secures Databases | **Find Vulnerabilities** | **Industry Best Practice**

1. Introduction
2. Cloud Computing Background
3. Challenges
4. Securing the Cloud
5. **Security Consolidation**
6. Q & A

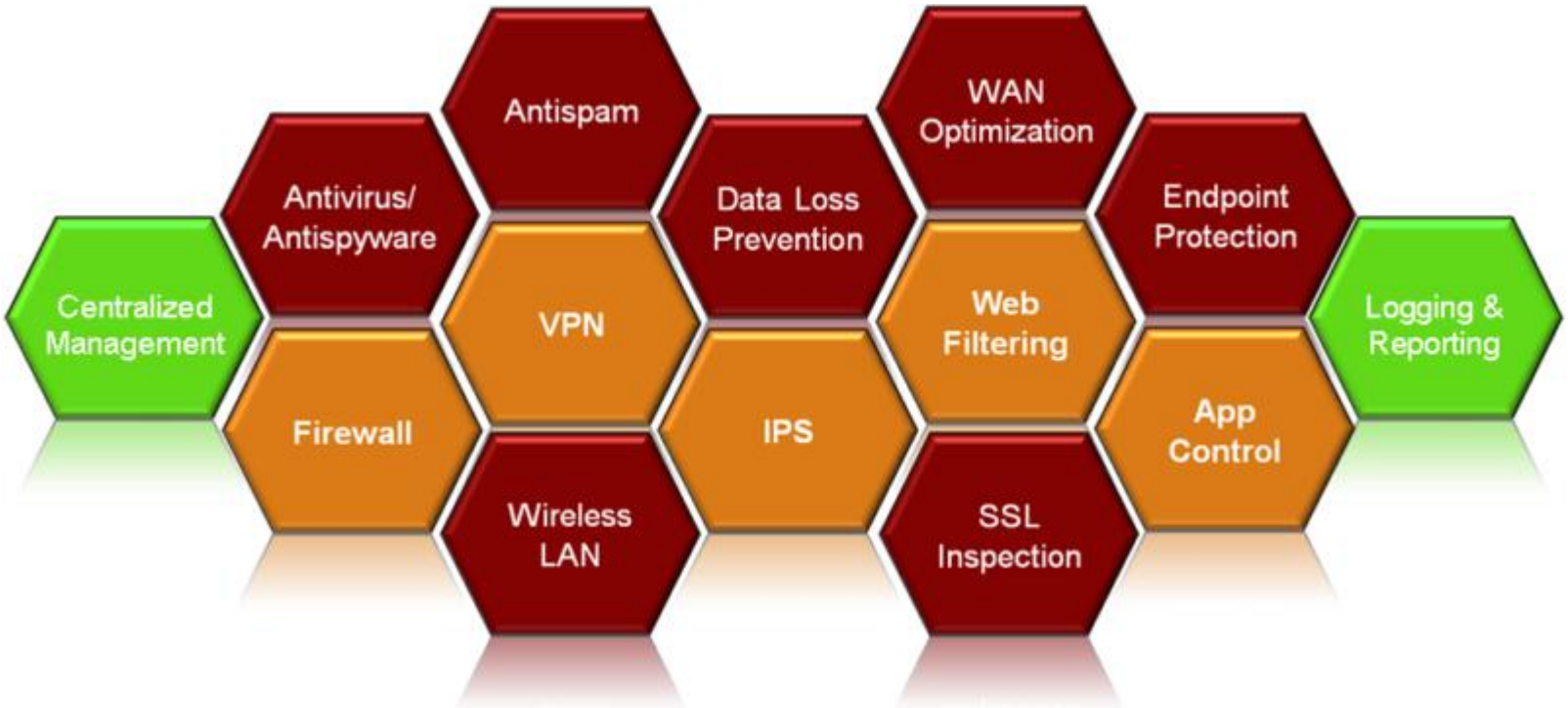
Multiple Threat Vectors

Threats can come from multiple parts of the cloud!

- E-Mail & Instant Messaging
  - Attachments: executable, archives AND documents
  - Links
- Web Sites
  - The “Drive-By Install” attack strategy
  - “Packs” available for purchase on the underground market
  - 2008: the year of SQL injections
- Social Networks
  - Intelligence source for targeted attacks
  - Worms (eg: Koobface)
- Physical Infection Vectors
  - Laptops
  - USB Keys
  - CDs

Security Consolidation

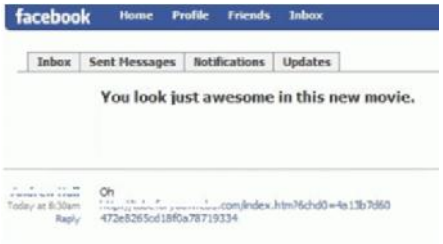
Goal: when facing a threat, be able to tackle it from different angles



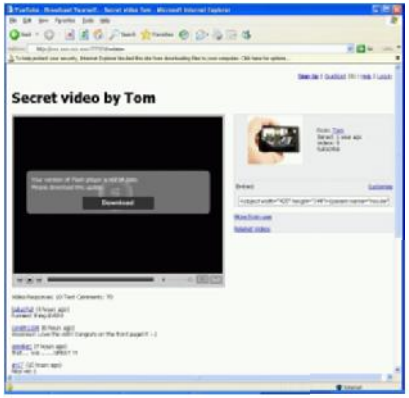
Solution must work together, simple, accurate and efficient

Security Consolidation in Action

Problem:



"Innocent" Video Link:
Redirects to malicious Website



"Out of date" Flash player error:
"Download" malware file

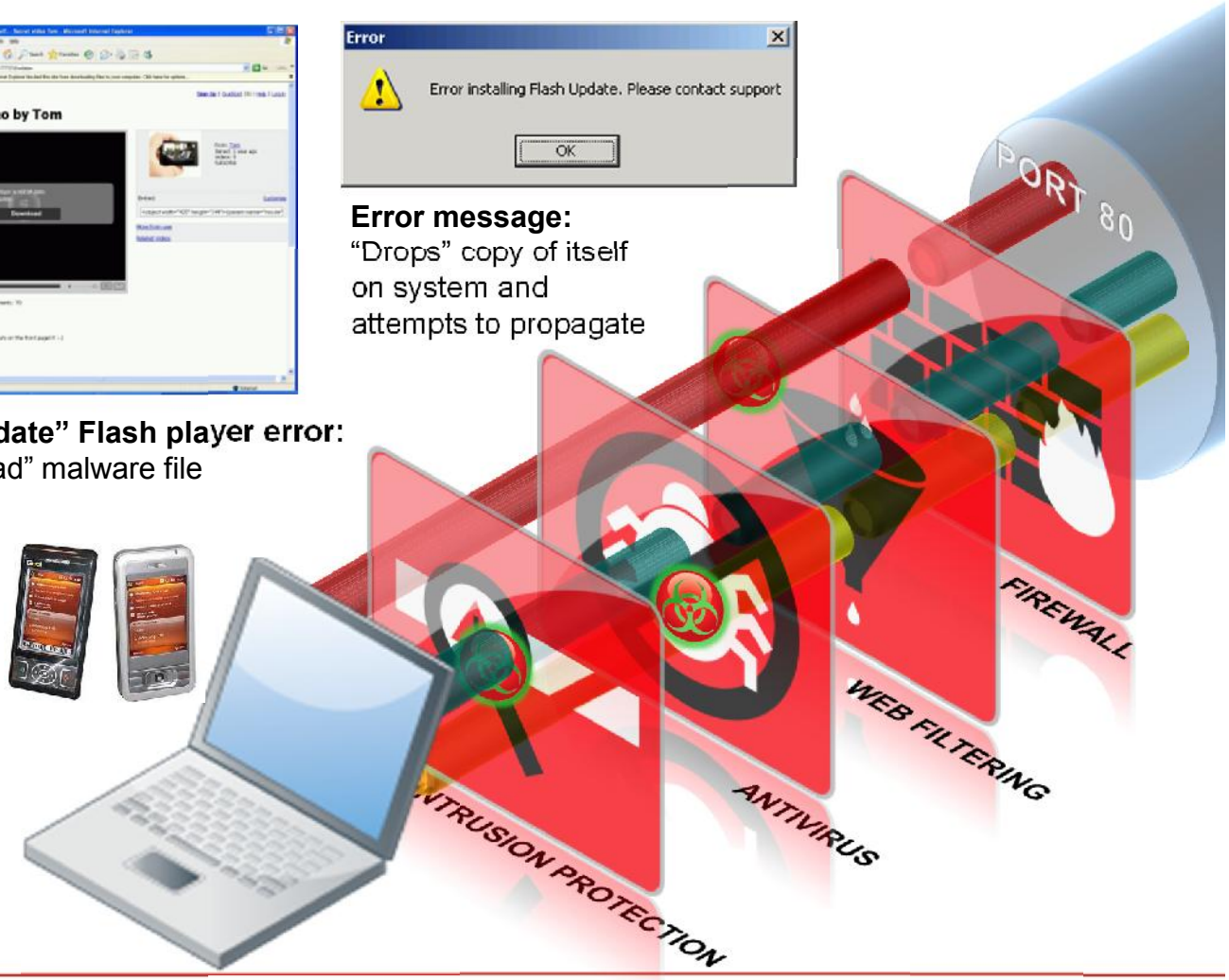
Error message:
"Drops" copy of itself on system and attempts to propagate

Solution:

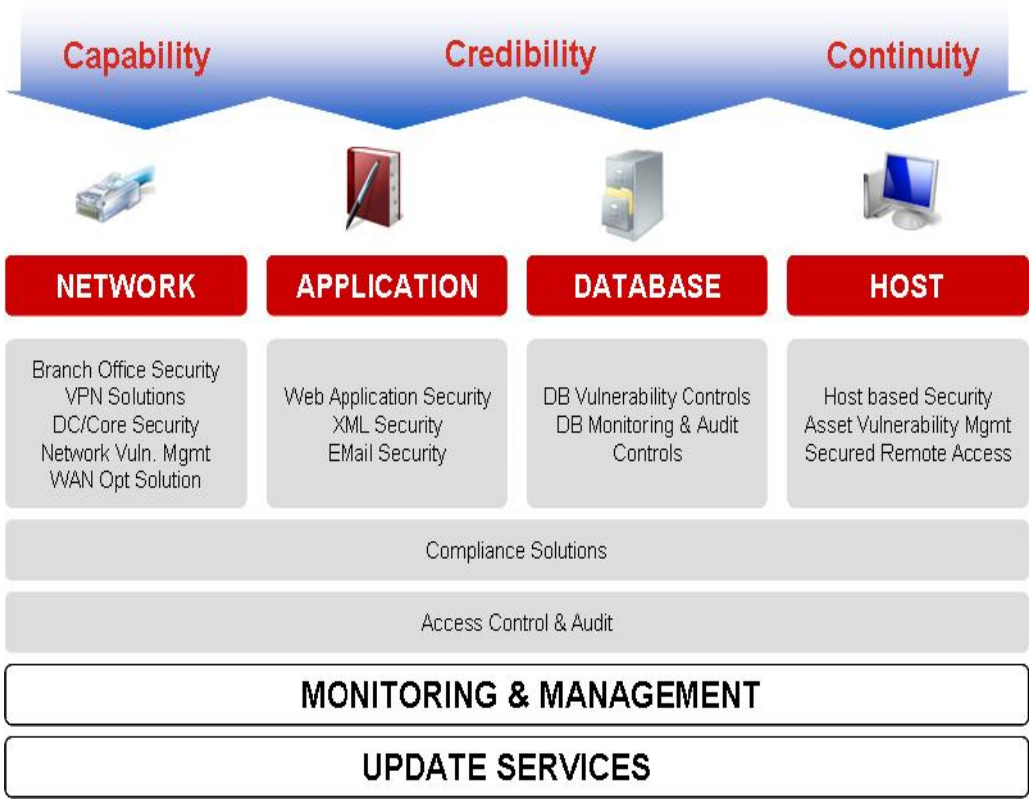
Integrated Web Filtering
Blocks access to malicious Website

Network Antivirus
Blocks download of virus

Intrusion Protection
Blocks the spread of the worm



Summary



- The cloud defines a new global business model
- It's here to stay …
- You need to fortify your assets in the cloud to protect your business
- Security Consolidation is needed to tackle multiple threats from different angles
- The cloud presents challenges, but at the same time opportunities if you build your IT security the way it should be done.

Questions

Thank You