



*Solutions to secure your network*

# Secure Cloud Utilization Strategies



Out of 127 cloud providers surveyed, a recently released study showed that only 25% of cloud providers surveyed consider cloud computing security as one of their most important responsibilities<sup>1</sup>.

# Secure Cloud Utilization Strategies

- Company and Individual Introduction
- What is the Cloud?
  - Cloud computing architectures
    - IaaS, PaaS, SaaS, etc.
  - Benefits, and potential issues
  - Mitigating security issues in the Cloud
- Security challenges and our solutions
  - SI Fortinet based Cloud security solution
  - Other SI Cloud security services

# Company Introduction

- Security Inspection, Inc. is a full service team of IT security experts providing:
  - Information Security
  - Virtualization Services
  - Private Cloud Services, Implementation Assessments, and Managed Cloud Security
  - Social Engineering
  - Vulnerability Assessments
  - Governance-Risk-Compliance

# What is the Cloud?

- Hosted applications
  - E-mail, collaboration, and storage
- Many consumer and enterprise offerings
  - Consumer: iCloud, Amazon S3, etc
  - Enterprise: Microsoft Azure, Red Hat CloudForms
  - For our purposes, we'll focus on enterprise
- Managed hardware and operating systems
  - Increase market leverage by reducing time to market, maintenance costs, and labor focus

# Cloud Computing Architectures

- Public cloud
  - Multi tenant environment leads to security concerns with non-public data
  - Less expensive, less secure
- Private cloud
  - Completely separate environment with respect to storage, hardware, and networking
  - More expensive, more secure
- Hybrid cloud
  - Combination of the above with sensitive data on private and public data in multi tenant environment
  - Varied pricing and security based on solution mix

# Benefits and potential issues

- Benefits of cloud architectures
  - Ease of access by users
  - Pay by usage models
  - Reduced maintenance costs, downtime, and labor
- Potential issues from reduced security focus
  - Ease of access also means increased exploitation vectors resulting from insecure networks
  - Easing maintenance also potentially means giving up control
  - Another Ponemon study estimates the average organizational cost of a data breach increased to \$7.2 million, an average of \$214 per compromised record<sup>3</sup>

# Risks of not securing data

- According to the CA/Ponemon survey, “[t]he majority of cloud providers believe it is their customer’s responsibility to secure the cloud and not their responsibility. They also say their systems and applications are not always evaluated for security threats prior to deployment to customers.”<sup>2</sup>
- Whose responsibility is cloud security?
  - Survey: 69% of cloud providers say it is the cloud users responsibility
  - Only 35% of the actual users believe it is their own responsibility
- Trend Micro survey: of 1,200 executives surveyed, 43% who are using cloud services have experienced a data security lapse or issue with cloud service<sup>4</sup>

# Mitigating Security Issues in the Cloud

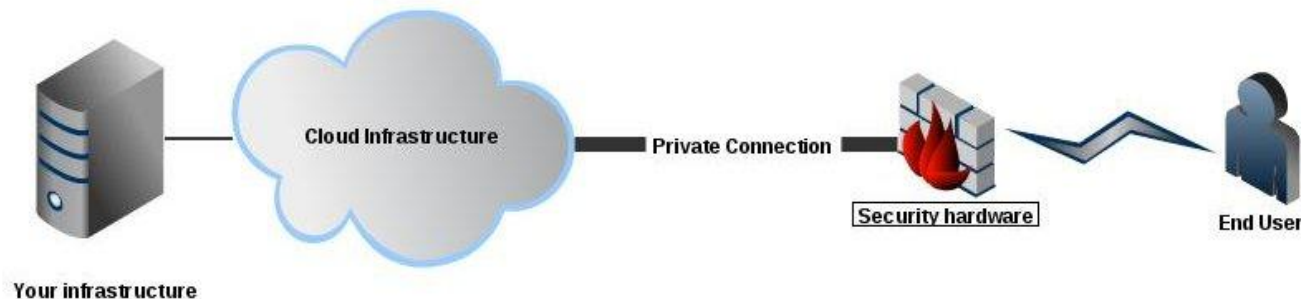
- Architecture and applications must provide four basic security features
  - Authentication - Is a user who they claim to be?
  - Authorization - Is a user authorized to perform attempted function?
  - Encryption
    - Removing the ability for “man-in-the-middle” situations (network)
    - If data is compromised or disseminated, ensure it is unusable without keys or algorithmic operations
  - Segmentation
    - In the event unauthorized access does occur, limiting access to the rest of your data/network

# Mitigating Security Issues in the Cloud

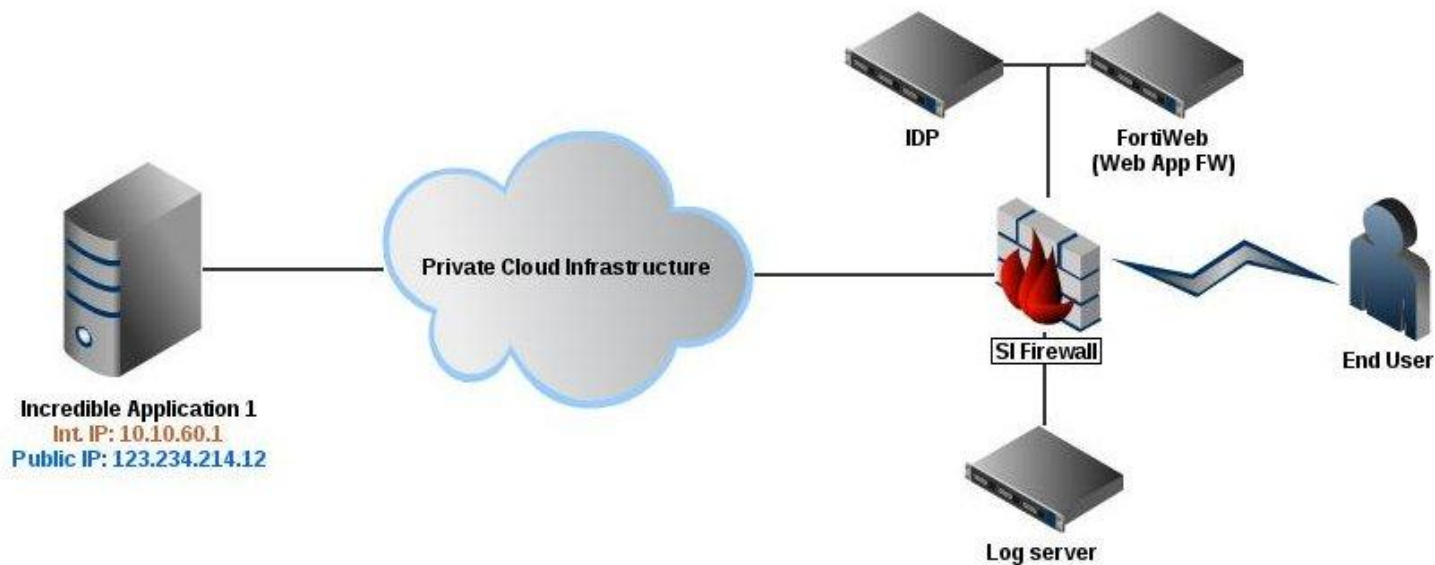
- For organizations bound to data handling standards, a fifth requirement is necessary
- Auditing of information system usage and data management
  - Solutions include software and hardware solutions such as GFI LANGuard and FortiAnalyzer
- To maintain compliance and competitive advantage, all of the above requirements should be met

# Mitigating Security Issues in the Cloud

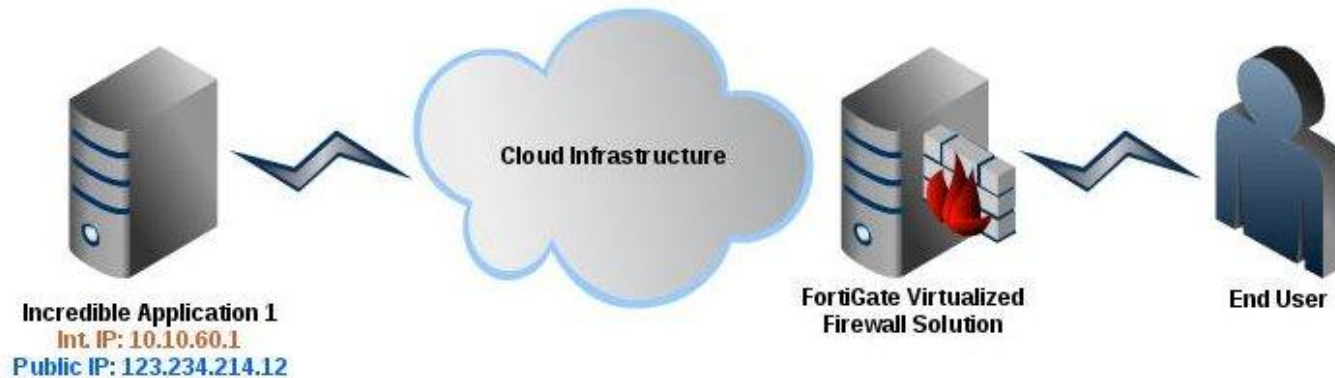
- Alternative network connectivity models
- Currently, many cloud based applications face directly toward the internet with limited security infrastructure
- Alternative model:



# Cloud Security Solution #1: Security as a Service



# Cloud Security Solution #2: Virtualized Firewall



# Other SI cloud security services

- Vulnerability assessments
  - Using industry standard applications, SI can provide systematic, documented vulnerability assessments
- Compliance auditing
  - Scheduled, comprehensive audits
  - Reporting for technical and management Executives

# Conclusion

- Maintaining a good security posture not only ensures the integrity of your data, but can also help avoid expensive litigation and loss of competitive advantage
- For more information, visit our web site at [www.securityinspection.com](http://www.securityinspection.com) or give us a call at 1 (855) SII-TECH.

# References

## **1: Security of Cloud Computing Providers Study by CA Technologies / Ponemon Institute**

Full document available online at:

<http://www.ca.com/~media/Files/IndustryResearch/security-of-cloud-computing-providers-final-april-2011.pdf>

## **2: Security of Cloud Computing Providers Study by CA Technologies / Ponemon Institute**

Full document available online at:

<http://www.ca.com/~media/Files/IndustryResearch/security-of-cloud-computing-providers-final-april-2011.pdf>

## **3: Ponemon Cost of a Data Breach by Symantec / Ponemon Institute**

Full document available online at:

[http://www.symantec.com/about/news/resources/press\\_kits/detail.jsp?pkid=ponemon](http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=ponemon)

## **4: Cloud Security Survey Global Executive Summary by Trend Micro**

Document available online at:

[http://es.trendmicro.com/imperia/md/content/uk/about/global\\_cloud\\_survey\\_exec\\_summary\\_final.pdf](http://es.trendmicro.com/imperia/md/content/uk/about/global_cloud_survey_exec_summary_final.pdf)