Cloud Security Concerns and the Perceived Effectiveness of Traditional Security Solutions in a Cloud Environment

Presented by: IDG Research
Company: CloudPassage
June 2015
METHODOLOGY & RESEARCH OBJECTIVES

Sample

Field Work
This survey was fielded from June 2, 2015 to June 12, 2015

Total Respondents
100 qualified completes

Method

Collection
Online Questionnaire

Number of Questions
10 (excluding screeners and demographics)

Audience
To complete this survey, respondents were required to hold a title of IT Director or above at a company with 1,000 or more employees. Respondents were also required to have involvement with or knowledge of their organization’s security as well as cloud initiatives and needs.

Survey Goals

The purpose of this survey is better understand cloud security concerns, particularly those related to customer data residing in the public cloud. We seek to understand perceptions of traditional security solutions as far as their effectiveness in a cloud environment. The survey also explores cloud deployment plans and adoption drivers.
RESPONDENT PROFILE

Total Respondents: 100

Organization Size:
- 10,000+ employees: 56%
- 1,000 – 9,999 employees: 44%

Top Represented Industries:
- Manufacturing, Production, Distribution: 20%
- Healthcare, Medical (hospitals, medical providers): 12%
- Computer related products or services: 11%
- Financial services (banking, accounting, tax, etc.): 11%
- Retail, Wholesale: 10%
- Insurance: 7%
- Business services, Consulting: 6%
- Education: 6%

Job Title Breakdown:
- CIO/CTO: 29%
- CSO/CISO: 10%
- Chief Architect: 4%
- Executive VP/Senior VP/VP of IT or IT Security: 13%
- Executive Director/Managing Director/Director of IT or IT Security: 45%
S3. How would you describe your involvement with or knowledge of your organization’s security initiatives and needs?
S4. How would you describe your involvement with or knowledge of your organization’s cloud initiatives and needs?

Base: 100 qualified respondents

Involvement with or knowledge of your organization’s security initiatives and needs

- Significant: 29%
- Moderate: 71%

Involvement with or knowledge of your organization’s cloud initiatives and needs

- Significant: 24%
- Moderate: 76%
KEY FINDINGS

• Respondents expect that IT services will increasingly be deployed in the cloud over the next 18 months (from 43% of IT services, on average, to 58%), with the most growth anticipated in public cloud deployments (from 12% to 20%). Agility and cost efficiency are the top drivers for cloud adoption at respondents’ organizations.

• Four in ten respondents (45%) report that the transition to cloud computing has made maintaining visibility into security and vulnerability more difficult. In fact, security concerns (cited by 66%) top the list of barriers impeding or stalling cloud infrastructure deployments. More than one third (37%) are concerned about the ability to meet compliance requirements.

• Respondents anticipate that 50% of customer data will reside in the cloud 18 months from now (nearly 20% in a public cloud).

• Half of all respondents (50%) are very concerned about the security of customer data residing in the public cloud, while another third (34%) are at least somewhat concerned. There are several factors contributing to concerns about the security of customer data that resides in the public cloud. Data ownership, location of data, and shared technology/multi-tenancy are cited by more than half of the respondents.

• The majority (80%) agree to some extent that conventional network (perimeter) security solutions don’t work well in cloud environments, and three-quarters (76%) agree their organizations lack visibility into attacks when applying traditional security in cloud infrastructure environments.

• Microsoft Azure is the cloud IaaS solution most often running in production today, followed by VMware vCloud Air and AWS. These are also the solutions that respondents’ organizations are most often testing and investigating.
SURVEY RESULTS
Agility and cost efficiency are the top drivers for cloud adoption at respondents’ organizations.

Q1. What are your organization’s top drivers for adopting cloud infrastructure (public, private, hybrid)? (Please select all that apply)
Base: 100 qualified respondents

- Improved agility/scalability: 74%
- Cost efficiencies: 67%
- Reduced IT overhead: 60%
- Faster time-to-market/speed of deployment: 55%
- Improved application performance: 46%
- Better data protection/security: 40%
- Other (please specify): 1%
Respondents expect that IT services will increasingly be deployed in the cloud over the next 18 months, with the most growth anticipated in public cloud deployments.

Q2. With the total equal to 100%, please indicate what percentage of your organization’s total IT services are delivered via traditional, private, public, and hybrid cloud, both currently and 18 months from now. Base: 100 qualified respondents.
Security concerns top the list of barriers impeding or stalling cloud infrastructure deployments. More than one third (37%) are concerned about the ability to meet compliance requirements.

**Barriers impeding cloud infrastructure deployments**

- Security concerns: 66%
- Reconfiguring systems/applications to be cloud-ready: 52%
- Lack of confidence in ability to meet compliance requirements: 37%
- Lack of in-house technical expertise: 34%
- Performance concerns: 29%
- Lack of executive buy-in: 24%
- Current cloud management tools do not support on-premises architecture: 23%
- Other (please specify): 1%
- None, we have no concerns: 4%
Four in ten (45%) report that the transition to cloud computing has made maintaining visibility into security and vulnerability more difficult.

The transition to cloud computing has made maintaining visibility into our security and vulnerability posture:

- Extremely difficult: 9%
- More difficult: 36%
- About the same: 33%
- Easier: 19%
- Much Easier: 3%

Q3. Please complete the following sentence: The transition to cloud computing has made maintaining visibility into our security and vulnerability posture:
Base: 95 respondents report some percentage of IT services are delivered via private, public, or hybrid cloud today
Respondents anticipate that 50% of customer data will reside in the cloud 18 months from now (nearly 20% in a public cloud).

Percentage of your organization’s customer data currently that resides on premise versus in the cloud

Q4. With the total equal to 100%, please indicate what percentage of your organization’s customer data currently resides in the following environments:
Base: 100 qualified respondents
Half of all respondents (50%) are very concerned about the security of customer data residing in the public cloud, while another third (34%) are at least somewhat concerned.

Q6. How concerned are you, or would you be, with the security of your customer data residing in the public cloud? Base: 100 qualified respondents
There are several factors contributing to concerns about the security of customer data that resides in the public cloud. Data ownership, location of data, and shared technology/multi-tenancy are cited by more than half of the respondents.

Factors driving security concerns regarding customer data residing in the public cloud:

- Data ownership: 56%
- Location of data: 51%
- Shared technology/multi-tenancy: 51%
- Virtual exploits: 47%
- Lack of strong access controls: 47%
- Insecure interfaces and APIs: 46%
- Shadow IT (i.e., individual business units deploying unsanctioned cloud workloads): 44%
- Distributed denial of service (DDoS) attack affecting performance/uptime: 41%
- Other (please specify): 3%

Q7. What are driving your security concerns with regards to customer data residing in the public cloud? (Please select all that apply)
Base: 100 respondents are very or somewhat concerned
Respondents estimate that it takes about 5 months, on average to procure and deploy a new security solution.
80% agree to some extent that conventional network (perimeter) security solutions don’t work well in cloud environments, and three-quarters (76%) agree their organizations lack visibility into attacks when applying traditional security in cloud infrastructure environments.

When it comes to applying traditional (non-cloud) security in cloud infrastructure environments:

- Strongly agree
- Agree
- Somewhat agree
- Somewhat disagree
- Strongly disagree

<table>
<thead>
<tr>
<th>Statement</th>
<th>% Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conventional network (perimeter) security solutions don’t work well in cloud environments</td>
<td>80%</td>
</tr>
<tr>
<td>Our security teams experience tool fatigue (i.e., number of tools is adding to complexity)</td>
<td>77%</td>
</tr>
<tr>
<td>We lack visibility into attacks</td>
<td>76%</td>
</tr>
<tr>
<td>We have difficulty gaining or maintaining compliance with regulations (e.g. PCI, HIPAA, etc.)</td>
<td>71%</td>
</tr>
<tr>
<td>Solutions take too long to procure and deploy</td>
<td>77%</td>
</tr>
<tr>
<td>We have too many point solutions</td>
<td>77%</td>
</tr>
<tr>
<td>Our solutions do not provide hardening and protection for each virtual server or workload</td>
<td>74%</td>
</tr>
<tr>
<td>Our solutions are difficult to scale</td>
<td>73%</td>
</tr>
</tbody>
</table>

Q8. Please rate your agreement with the following statements: When it comes to applying traditional (non-cloud) security in cloud infrastructure environments:
Base: 95 respondents report some percentage of IT services are delivered via private, public, or hybrid cloud today
Microsoft Azure is the cloud IaaS solution most often running in production today, followed by VMware vCloud Air and AWS. These are also the solutions that respondents’ organizations are most often testing and investigating.

### Organization’s usage of IaaS vendors

- **Microsoft Azure**
  - Running in production environment: 36%
  - Experimenting in test and development: 26%
  - Exploring, researching, and investigating solutions: 19%
  - No immediate plans to use: 19%

- **VMware vCloud Air** (formerly VMware vCloud Hybrid Service)
  - Running in production environment: 29%
  - Experimenting in test and development: 26%
  - Exploring, researching, and investigating solutions: 23%
  - No immediate plans to use: 22%

- **Amazon Web Services (AWS)**
  - Running in production environment: 28%
  - Experimenting in test and development: 18%
  - Exploring, researching, and investigating solutions: 30%
  - No immediate plans to use: 24%

- **IBM Cloud**
  - Running in production environment: 20%
  - Experimenting in test and development: 20%
  - Exploring, researching, and investigating solutions: 17%
  - No immediate plans to use: 43%

- **Google App Engine**
  - Running in production environment: 7%
  - Experimenting in test and development: 20%
  - Exploring, researching, and investigating solutions: 20%
  - No immediate plans to use: 52%

Q10. Which of the following best describes your organization’s usage of the following cloud IaaS vendors? Base: 95 respondents report some percentage of IT services are delivered via private, public, or hybrid cloud today.
S1. Approximately how many people are employed in your entire organization or enterprise? (Please include all plants, divisions, branches, parents and subsidiaries worldwide)
D2. Which of the following best describes your organization's industry or function?
Base: 100 qualified respondents