

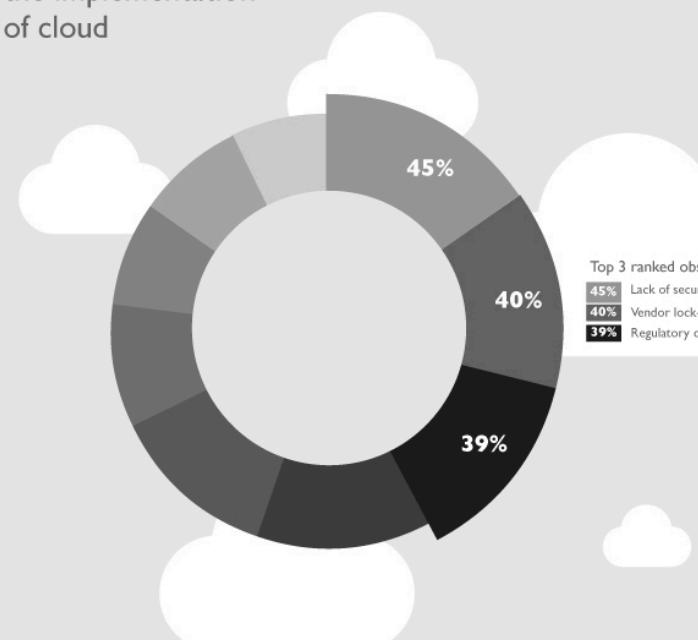
Cloud Security

Outline

- Understanding Cloud Security
- Most common risk, threats, and vulnerabilities of Cloud-based services and hosted solutions
- Precautionary steps to take note of

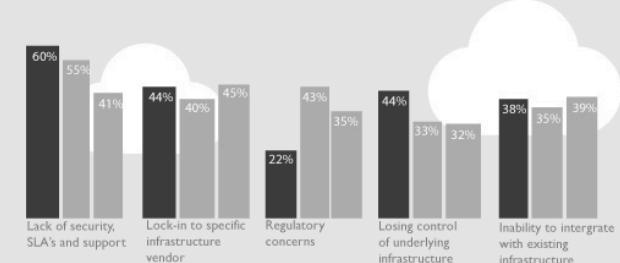
Security is the major concern

Biggest obstacles
when it comes to
the implementation
of cloud

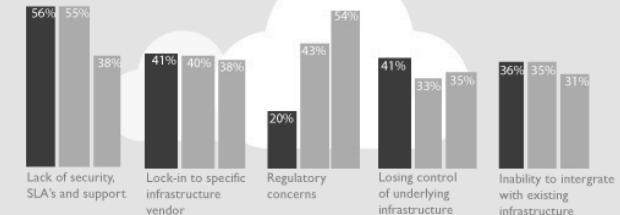


Top 3 ranked obstacles
45% Lack of security and SLA
40% Vendor lock-in
39% Regulatory concerns

Biggest obstacles
when it comes to
the implementation
of cloud per
business size



Biggest obstacles
when it comes to
the implementation
of cloud per
involvement level

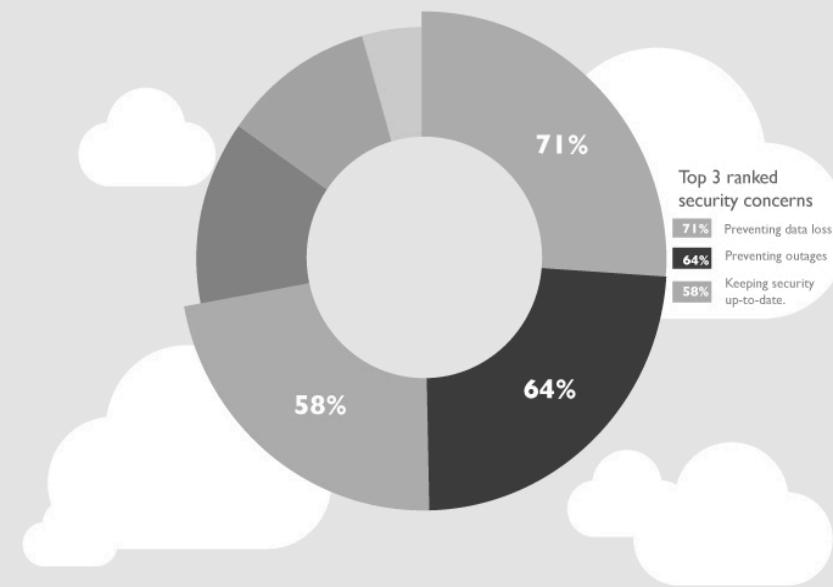


interxion

Source: <http://www.interxion.com/cloud-insight/>

Main security concerns

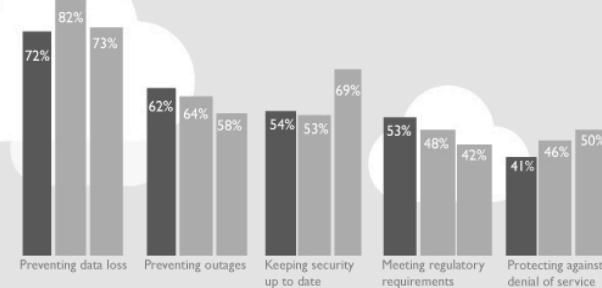
What is your biggest security concern with cloud computing?



Biggest security concern with cloud computing per business size



Biggest security concern with cloud computing per involvement level



interxion

Source: <http://www.interxion.com/cloud-insight/>

General security challenges

- Wide range of architectures: proprietary implementations cannot be examined!
 - Trusting the vendor's security model
- Loss of physical control
- Data separation / protection
- Authentications
-

Security issues

- ***Key issues:***
 - Country or jurisdiction
 - Multitenant risks
 - Malicious insiders
 - Vendor lock in
 - Cloud-based provider failing
- **Relevant components**
 - Processing infrastructure
 - Provisioning services
 - Data Storage services
 - Support services
 - Network and perimeter

On the plus side...

- Data fragmentation and dispersal
- Hypervisor protection against network attacks
- Fault tolerance, better reliability
- Real-time detection of system tampering.
- Greater investment in security infrastructure
- On-demand security controls
- Immediate deployment of software patches
- Hardware and software redundancy
- Timeliness of incident response
- Specialists instead of personnel

Main threats

- Main threats:

- Shared Technology Vulnerabilities
- Insecure Interface and APIs
- Abuse and Malicious use of Cloud Services
- Data Loss/Leakage
- Data Breaches
- Account or Service Traffic Hijacking
- Denial of Service
- Malicious Insiders
- Unknown Risk Profile!
- ...

Shared resources

- Underlying components that make up cloud infrastructure (CPU caches, GPUs, etc.) were not designed to offer strong isolation properties for a multi-tenant architecture
- Is the hypervisor secure enough? Is it possible to access the host / other guests from a guest virtual machine instance?
 - Kortchinsky's CloudBurst presentations (A VMware Guest to Host Escape Story): Hypervisors have exhibited flaws that have enabled guest OSs to gain inappropriate levels of control or influence on the underlying platform
 - Hyperjacking attack

IaaS

PaaS

SaaS

What was that escape story?

- A memory-corruption exploits of drivers vulnerabilities (emulated graphics driver) demonstrated the possibility of a host infiltration from the guest
 - Guest VM can write data in the host process memory and execute malicious code on host. It was patched after the exploit release
- Other simpler escape methods were also reported, such as host file system directory traversal

Abuse and malicious use of resources

- Access, registration and usage models of the clouds facilitates anonymity and can lead to
 - Spammers
 - Hosting malicious data and running malicious code
 - Launching dynamic attack points
 - Botnet command and control
 - DDOS
 - ...

IaaS	PaaS	SaaS
------	------	------

Insecure interfaces and APIs

- The security of APIs and interfaces (browsers...), for provisioning, management, and monitoring
 - Authentication types and data encryption
 - Access control, anonymous access
 - Unsecure Mashups
 - Limited monitoring and logging capabilities
 - API dependencies
 - ...

IaaS	PaaS	SaaS
------	------	------

<http://www.programmableweb.com/> (lists 5000+ APIs, mashups, codes, etc.)

Data loss, leakage, and integrity risks

- The threat of data compromise increases in the cloud, due to its architectural or operational characteristics. There are many ways to compromise data, including
 - Deletion or alteration of records without backups, unlinking records, etc.
 - Loss of an encoding key may result in effective destruction
 - Inconsistent use of encryption and software keys
 - Unauthorized access to sensitive data
 - Jurisdiction and political issues
 - ...

IaaS	PaaS	SaaS
------	------	------

Encryption

- Encryption can be a solution to secure access (OS, applications) and data protection, traffic, etc.
 - Computations can be done on encrypted data, but it can have a large overhead
- There are no efficient search capabilities on encrypted data
- Today's cryptography still lacks the expressive power to efficiently support outsourcing to potentially untrusted clouds

Data security and storage

- **Data security at all levels (SaaS, PaaS, IaaS):**
 - Data-in-transit
 - Data-at-rest
 - Processing of data, including multi-tenancy
 - Data lineage
 - Data provenance
 - ...
- **NOT all of these data security facets are of equal importance in all topologies – private / public clouds, sensitive / non-sensitive data...**

Data-in-transit

- Primary risk: not using a vetted encryption algorithm,
- It is very important to ensure that a protocol provides confidentiality as well as integrity:
 - SCP, FTP over SSL/TLS...
- Encrypted data using a non-secured protocol (e.g. FTP or HTTP) can provide confidentiality but does not ensure the integrity of the data.

Privacy Preserving Data Analytics

- **What is Privacy?**

- “Freedom from unauthorized intrusion” (*Merriam – Webster*)

- **Does Data Analysis pose a privacy risk?**

- **Infrastructures:** misuse

- Complete, comprehensive and accurate datasets

- **Results**

- isolate an individual and determine private information

- **Solutions**

- Models and techniques about aggregated data without direct access to all detailed information of individual transactions

- Cannot be traced to an individual

Privacy Preserving Techniques: Transformation

- Privacy-preserving clustering
- Isometric transformation:
 - $T: \mathbb{R}^n \rightarrow \mathbb{R}^n$
 - $|T(p) - T(q)| = |p - q|, \forall p, q \in \mathbb{R}^n$
- Special cases: translation, rotation...
- Rotation of a point in 2D:
$$v_r = R \times v$$
 - v : vector column containing the original coordinates
 - v_r : vector column containing the rotated coordinates

$$R = \begin{bmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{bmatrix}$$

Transformation (II)

• Rotation-Based Data Perturbation

- Data sets $D_{m \times n}$, m objects of n attributes
- $D_r = f_r(D)$: $\forall i, j : 1 \leq i, j \leq n, i \neq j, A_i, A_j \in D, A_i^r, A_j^r \in D_r$
 - $V(A_i, A_j) \rightarrow V_r(A_i^r, A_j^r)$ by $V_r = R \times V$
- Pair wise security threshold:
 - $\text{Variance}(A_i - A_i^r) \geq \rho_1$ and $\text{Variance}(A_j - A_j^r) \geq \rho_2$ with $\rho_1, \rho_2 > 0$

ID	age	weight	heart_rate
1237	75	80	63
3420	56	64	53
2543	40	52	70
4461	28	58	76
2863	44	90	68

$$\theta = 312.47$$

ID	age	weight	heart_rate
1237	-1.4405	0.0819	0.8577
3420	-1.0063	1.0077	-0.7108
2543	1.1368	0.5347	-0.0429
4461	1.7453	-0.3078	-0.0701
2863	-0.4353	-1.3165	-0.0339

Data lineage / provenance

- Lineage - Following the path of data
- Providing data lineage to auditors is time-consuming but important for an auditor's assurance
- Accurate reporting on data lineage for a public cloud service is almost impossible
 - Example: data have been transferred to a cloud provider (e.g. AWS) at date x_1 , at time y_1 , then processed (e.g. By EC2) at date x_2 , at time y_2 , and restored in another bucket (e.g. on Amazon's S3) and finally transferred back to the organisation for storage in a internal data warehouse at date x_3 , at time y_3 .
- Data provenance: not only that the data has integrity but also that it is computationally accurate

Account or Service Hijacking

- As applies to traditional systems and web services
 - Phishing / Stolen credentials
 - Data manipulation
 - Services redirection
 - Return falsified information
 - Exploitation of software vulnerabilities
 - ...

IaaS	PaaS	SaaS
------	------	------

Unknown risk profile!

- Applications depends (critically!) on the trustworthiness of your cloud providers
- Security by obscurity may be low effort, but it can result in unknown exposures. It may also impair the in-depth analysis required highly controlled or regulated operational areas
- Information about who is sharing your infrastructure, network intrusion logs, redirection attempts and/or successes, and other logs, may all be pertinent

IaaS	PaaS	SaaS
------	------	------

Gartner's list

- **Privileged user access:** Inquire about who has specialised access to data, and about the hiring and management of such administrators.
- **Regulatory compliance:** Make sure that the vendor is willing to undergo external audits and/or security certifications.
- **Data location:** Does the provider allow for any control over the location of data?
- **Data segregation:** Make sure that encryption is available at all stages, and that these encryption schemes were designed and tested by experienced professionals.

Gartner's list

- **Recovery:** Find out what will happen to data in the case of a disaster. Do they offer complete restoration? If so, how long would that take?
- **Investigative support:** Does the vendor have the ability to investigate any inappropriate or illegal activity?
- **Long-term viability:** What will happen to data if the company goes out of business? How will data be returned, and in what format?