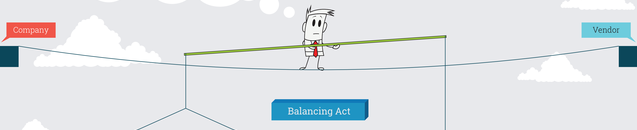
How to Secure Your IaaS and PaaS Environments

Keep your information security risks manageable when leveraging the benefits of cloud computing.

If you want to take advantage of any of the public IaaS or PaaS benefits, you have to secure your new environment. To ensure data protection and secure operations from creation to decommission, you have to achieve control, visibility, data security, management, and compliance.

The ability to secure expanding operating environments, such as the cloud, is a core responsibility of security professionals. Organizations must be able to take advantage of the latest technological capabilities without putting their enterprise or information at unreasonable risk. The person in charge of security at the organization must ensure that IT can enable business objective realization in a secure and safe way.



Balancing Act

Securing an IaaS or PaaS environment is a balancing act of determining whether the vendor or the consumer is responsible for meeting specific security requirements.

Security Perception

The cloud can be secure although unique security threats and vulnerabilities cast concerns to consumers.

It becomes your job to determine the balance of power. This includes the responsibility of the security control itself (whether policy, process, or technology), the responsibility of verifying the control, the responsibility of providing auditing of the control, and the responsibility of maintaining the control.

Structured CSP Selection Process

Most security challenges and concerns can be minimized through a structured process of selecting a trusted cloud service provider partner.

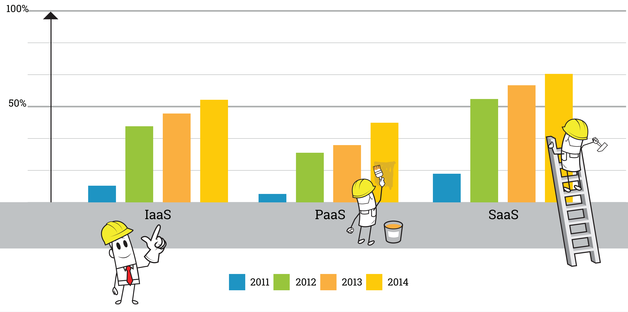
Cloud Security Alliances's "Nine Notorious Cloud Security Risks":

1. Data breach
2. Data loss
3. Account of service traffic hijacking
4. Insecure interfaces and APIs
5. Denial of service
6. Malicious insiders
7. Cloud abuse
8. Insufficient due diligence
9. Shared technology vulnerabilities

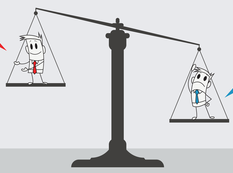
Source: https://cloudsecurityalliance.org/research/top-threats/

Approximately **66%** of data is in the cloud today, and **49%** of companies are using cloud to fuel revenue generation or new product creation.

The types of cloud computing technologies organizations are using



Security remains the biggest concern. Despite declining slightly in 2013, it rose again as an issue in 2014 and was cited by **49%** of respondents.



Privacy is of growing importance. As an inhibitor, privacy grew from 25% in 2011 to 31% in 2014.

Over 1/3 of respondents see regulatory/compliance as an inhibitor to moving to the cloud.

Steps for Success

Step 1
Determine your hosted IaaS/PaaS specific risk profile

IaaS and PaaS present unique security risks and threats compared to traditional physical infrastructure. Determine your organization's overall IaaS/PaaS risk profile.

Your hosted cloud risk profile is based on:

- Industry profile
- Organization type
- Data
- Compliance
- Systems moving to the cloud
- Threats
- Current risk management
- User community size

Step 2
Determine your cloud security control requirements

Various security controls must be accounted for within a cloud environment. From your risk profile, determine what security controls your IaaS/PaaS program needs, as well as whether your vendor or you will be responsible for their deployment.

Info-Tech's custom cloud security framework is the CAGI model:

- Completeness of security controls
- Auditability of cloud environment
- Governability of cloud environment
- Interoperability of cloud system

Step 3
Evaluate your vendors from a security perspective

Now that you have determined all of your SLA requirements and documented them in your security SLA, it's time to identify vendors that have satisfied these requirements and start talking.

Vendor selection and relationship management is an extremely long process - start talking now to get things going!

Step 4
Implement your hosted cloud security controls

Implement identified security controls through in-depth implementation steps for each control.

Identify potential obstacles and stakeholders, develop your implementation roadmap, and create a communication plan to ensure successful adoption and buy-in.

Step 5
Build a Cloud Security Governance Program

Build an IaaS/PaaS security governance plan to manage your vendor to ensure a successful relationship and continued security, in addition to ensuring your internal controls are maintained and secured.

"The key challenges are process related, policy related, and culturally related. These are the most difficult to change."
– Steve Woodward, CEO, Cloud Perspectives