EXECUTIVE SUMMARY

Securosis

What CISOs Need to Know About Cloud Computing

Cloud is Different, but Not the Way You Think

There is no question cloud computing is fundamentally changing how we deliver and consume technology resources, but the main impacts to security are not outsourcing or sharing infrastructure with others. Cloud computing doesn't necessarily reduce security risks, it shifts them.

- Cloud computing is a radically different technology model – not just the latest flavor of outsourcing. It uses a combination of *abstraction* and *automation* to achieve previously impossible levels of efficiency and elasticity. But in the end cloud computing still relies on traditional infrastructure as its foundation.
- Between business benefits and current adoption rates, *we expect cloud computing to become the dominant technology model over the next ten to fifteen years*. As we make this transition it is the technology that creates clouds, rather than the increased use of shared infrastructure, that really matters for security.
- *Multitenancy is more an emergent property* of cloud computing than a defining characteristic, despite being the trait many security professionals become distracted by.
- It is ***Abstraction*** *and* ***Automation*** that impact security more than multitenancy or outsourcing in cloud computing.
- **Abstraction** separates resources from the underlying infrastructure.
  - Your entire (cloud) infrastructure is now managed over the network using web interfaces and APIs. This *management plane* provides remote, complete, control over your infrastructure.
  - Security may lose visibility since we can't rely on physical network routing or asset management. We don't even necessarily know which exact hard drives hold which data.
  - Everything is virtual and portable. Entire servers can migrate to new physical systems with a few API calls or a click on a web page.
  - Compliance may be more complex due to less knowledge of where things are located, and auditors who don't understand cloud computing technologies.
- **Automation** uses *orchestration* technologies to manage provisioning and configuration of resources based on policies.
  - Security compliance is easier to automate, since everything runs through the cloud controller. *This reduces certain security risks*.
  - The environment is highly dynamic, with servers appearing and disappearing on-demand. Manual security controls or non-continuous assessments can't keep up.
  - You *gain greater governance and visibility* of your infrastructure, since the orchestration layer knows where everything is, at all times, and how it is configured.

Here are some examples of how cloud is different:

CSA cloud security alliance SM

This content of this independently created paper has been reviewed and approved by the Cloud Security Alliance. *It does not imply endorsement of any specific vendors or products.* Securosis would like to thank the CSA for their support in reviewing the content.

This is an executive summary of the complete paper, *What CISOs Need to Know About Cloud Computing* by Rich Mogull, Securosis LLC

- **Autoscaling:** Monitoring tools in the cloud automatically launch new virtual servers based on templates to meet demand, then delete them when load drops. No human IT admin needed.
- **Immutable Servers:** Instead of patching servers, some organizations use the same techniques to launch new, up to date servers and delete the old ones. Even on live applications with users connected, thanks to new application architectures.
- **Snapshots:** A snapshot is a near-instant backup of all the data on a cloud storage volume, without taking the system down or affecting performance. These snapshots are incredibly portable and, in public clouds, can be made public.
- **Management Credentials:** The entire infrastructure deployed on the cloud is managed, even down to the network and server level, using API calls and web interfaces. Configured incorrectly, someone can own your datacenter by hacking an admin's personal laptop.
- **Software Defined Security:** Security can use these same features and APIs to automate security controls, and tightly integrate with the infrastructure. New servers automatically deploy with secure configurations, and you can instantly identify all digital assets.

Adapting Security for Cloud

Cloud computing poses new risks, while both increasing and decreasing existing risks. The trick is to leverage the security advantages, freeing up resources to cover the gaps. Start with Five general principles, all of which we see used today:

- *You cannot rely on boxes and wires*. Networks are virtual, so you can't put physical security devices inline, and virtual security tools behave differently.
- *Security should be as agile and elastic as the cloud itself.* Your security tools need to account for the highly dynamic nature of the cloud, where servers might pop up automatically and run for only an hour before disappearing forever.
- *Rely more on policy-based automation.* Wherever possible design your security to use the same automation as the cloud itself.
- *Understand and adjust for the characteristics of the cloud.* Take advantage of the native automation and orchestration of the cloud to embed security. By, for example, inserting security agents into virtual servers that automatically connect and self configure.
- *Integrate with DevOps*. Not all organizations are using DevOps, but DevOps principles are pervasive in cloud computing. Security teams can integrate with this approach and leverage it themselves for security benefits.

Real-World Examples

Here are a few examples of cloud security used in production environments today:

- Applications stacks are *hypersegregated* as the cloud platform places a virtual firewall around every single server, making it nearly impossible for an attacker to spread internally.
- Cloud-aware security agents are automatically embedded in every virtual machine as they launch. They then automatically configure themselves based on policies and the environment.
- Administrator access to the cloud management plane runs through security proxies to monitor all infrastructure changes.
- *Software Defined Security* programs constantly monitor the entire cloud for policy violations. They can automatically fix configurations and quarantine systems, or identify system owners and recommend changes.

This report is licensed by CloudPassage. All content was developed independently.

CloudPassage

CloudPassage is the leading cloud infrastructure security company. Based on a next-generation security-as-a-service architecture, CloudPassage Halo was purpose built to automate security and compliance in any private, public, or hybrid cloud, or data center.

www.cloudpassage.com