KASEY PANETTA

MARCH , 27, 2018
GARTNER.COM

TECHNICAL WHITEPAPER

IS THE CLOUD SECURE?

TABLE OF CONTENTS

Recommendations for Developing a Cloud Computing Strategy and Predictions for the Future of Cloud Security P. 3

Develop an Enterprise Cloud Strategy P. 3

Build Expertise in Your Cloud Models P. 4

Act on Cloud Predictions P. 5

RECOMMENDATIONS FOR DEVELOPING A CLOUD COMPUTING STRATEGY AND PREDICTIONS FOR THE FUTURE OF CLOUD SECURITY.

In a world where security breaches dominate the headlines, the ambiguity that surrounds cloud computing can make securing the enterprise seem daunting. Concerns about security have led some CIOs to continue inhibiting their organizational use of public cloud services.

The challenge exists not in the security of the cloud itself, but in the policies and technologies for security and control of the technology. In nearly all cases, it is the user — not the cloud provider — who fails to manage the controls used to protect an organization's data.

"Through 2022, at least 95% of cloud security failures will be the customer's fault"

"CIOs need to ensure their security teams are not holding back cloud initiatives with unsubstantiated cloud security worries," says Jay Heiser, research vice president at Gartner. "Exaggerated fears can result in lost opportunity and inappropriate spending."

CIOs must change their line of questioning from "Is the cloud secure?" to "Am I using the cloud securely?" Heiser helps CIOs find the right answers and solutions to this question with recommendations for developing a cloud strategy and predictions for the future of cloud security.

DEVELOP AN ENTERPRISE CLOUD STRATEGY

First obtain consensus from the leadership team. All members need to agree that cloud computing has become indispensable and that it should be governed through planning and policy. This is the most significant step to ensure appropriate levels of cloud security.

"Different cloud models have different risk and control ramifications. Make sure your strategy reflects this reality"

"Gartner clients who have made explicit executive decisions on their cloud strategy are providing far more guidance to the business and IT," explains Heiser. Increased guidance allows for:

- **Better requirement analysis**

- **More sophisticated architectural planning**
- **More flexible risk acceptance processes**

The enterprise strategy should outline the organizational expectations for the form, significance and control of public cloud. This gives CIOs a clear mandate to influence the use of public clouds on behalf of business units. The strategy should also include guidance on what data can be placed into which clouds under what circumstances.

BUILD EXPERTISE IN YOUR CLOUD MODELS

Different cloud models have different risk and control ramifications. Make sure your strategy reflects this reality. It should also ensure that staff assigned to strategically important use cases have the skills required to do so with security and compliance. In most cases, your team will need to be proficient in both infrastructure as a service (IaaS) and software as a service (SaaS) models.

The basic deployment and operational framework of IaaS is broadly the same as the processes and skills used in traditional IT. Yet, it calls for security and operational teams to acquire a specific set of skills:

- **Virtualization and CSP-specific knowledge**
- **Identity and access management**
- **Workload protection**
- **Network security and encryption**

CIOs who want to use IaaS for sensitive use cases need to ensure their teams have a sophisticated understanding of cloud-specific security technologies and know how to leverage the programmatic infrastructure of IaaS providers for security automation.

> **“CIOs should encourage their teams to apply imagination and energy to develop new approaches to securely and reliably leverage the benefits of IaaS, SaaS and platform as a service”**

In contrast, the entire SaaS technology stack is under the direct control of the service provider. This means that to govern SaaS usage, CIOs must focus on Identity and Access Management (IAM) permissions management and the protection of sensitive data. This is accomplished by relying on whatever mechanisms each SaaS provider makes available or by use of a third-party product, such as a cloud access security broker (CASB).

As overseeing SaaS demands less technical expertise, there is a wide range of roles that can manage it:

- **IT operations**
- **IT security**
- **The compliance or privacy function**
- **The business units**

ACT ON CLOUD PREDICTIONS:

- **In 2018, the 60% of enterprises that implement appropriate cloud visibility and control tools will experience one-third fewer security failures.** Placing workloads in the cloud does not require a security trade-off. Enterprises actually benefit from the security built into the cloud. “CIOs should encourage their teams to apply imagination and energy to develop new approaches to securely and reliably leverage the benefits of IaaS, SaaS and platform as a service (PaaS),” says Heiser.
- **Through 2020, public cloud infrastructure as a service (IaaS) workloads will suffer at least 60% fewer security incidents than those in traditional data centers.** CIOs should look to leverage the programmatic infrastructure of public cloud IaaS. Automating as much of the process as possible will remove the potential for human error — generally responsible for successful security attacks. Enterprise data centers could also be automated, but usually don’t offer the programmatic infrastructure required.
- **Through 2022, at least 95% of cloud security failures will be the customer’s fault.**CIOs can combat this by implementing and enforcing policies on cloud ownership, responsibility and risk acceptance. They should also be sure to follow a life cycle approach to cloud governance and put in place central management and monitoring planes to cover the inherent complexity of multicloud use.