COMCAST BUSINESS | MASERGY

WHAT YOU'LL LEARN

- The impact of IaaS/PaaS on your security focus
- Your responsibilities under shared security models
- A security analysis of IaaS/PaaS vs. on-premise environments

E - GUIDE

How to secure IaaS/PaaS effectively: customer responsibilities in the shared security model

Cloud computing offers significant advantages to IT, but securing Infrastructure-as-as-Service (IaaS) and Platform-as-a-Service (PaaS) require the right strategy, controls, and monitoring. In the shared security model, here's how customers should shift their focus.

From a security perspective, what changes when migrating to IaaS/PaaS?

Fundamentally, none of the security essentials change when migrating to cloud computing. Rather, what changes is the security focus of the IaaS/PaaS tenant -- in other words you, the enterprise customer. In the IaaS shared security model, the IaaS provider assures security of the virtual machines, disks & storage and networking, while the IaaS tenant is responsible for security of the operating system, software stack, and data. The IaaS tenant must now focus on what he or she can control, but must also trust (and verify) that the IaaS is doing its job correctly. This bifurcation of responsibilities is good because the IaaS tenant's limited security resources will now go a lot further in reducing overall risk.

Shared Security Models for Cloud

Responsibility	SaaS	PaaS	IaaS	On-Prem
Data	Enterprise	Enterprise	Enterprise	Enterprise
Account & Access Controls	Enterprise	Enterprise	Enterprise	Enterprise
Identity & Access Management (IAM)	Enterprise	Enterprise	Enterprise	Enterprise
Application	Cloud	Enterprise	Enterprise	Enterprise
Network Virtualization	Cloud	Enterprise	Enterprise	Enterprise
Operating System	Cloud	Cloud	Enterprise	Enterprise
Virtualization	Cloud	Cloud	Cloud	Enterprise
Hardware (Servers + Storage)	Cloud	Cloud	Cloud	Enterprise
Networking	Cloud	Cloud	Cloud	Enterprise
Physical Infrastructure	Cloud	Cloud	Cloud	Enterprise

Enterprise / Cloud Tenant oud Provider

Is IaaS/PaaS more or less secure than on-premise environments?

A few years ago, the enterprise perception was that cloud computing environments were less secure than on-premise environments. The reality is that for all organizations (except perhaps the most well resourced large ones) IaaS has the ready-potential to be substantially more secure than on-premise environments. Security is an overhead cost, and big organizations with big budgets can spend much more money and time than mid-sized organizations to do security correctly.

This trend extends to IaaS/PaaS providers who have the most extensive security budgets and world-class security teams with state-of-the-art security tools and processes. As long as the tenant picks a reputable IaaS/PaaS provider and focuses on what they should be controlling, they will improve their security. This last point is critical because if the IaaS tenant does not do their part, the whole security model will fail.

What should IaaS/PaaS customers do to secure their part of the shared security model?

There are a number of controls and best practices you should put in place. Here are some key ones (in no particular order):

- Lock down root account credentials and create access groups and users with limited privileges (based on job responsibilities). Monitor all access 24/7 for suspicious activity.
- Remove unneeded software and applications from workload images and harden through configuration settings. Monitor 24/7 for any configuration drift.
- Scan production workloads in real-time for vulnerabilities and kill instances deemed risky. Replace with new workloads based on the patched image
- Segment network traffic using Virtual Private Clouds and host firewalls. Monitor traffic for malicious activity.
- Encrypt data-at-rest and data-in-motion and monitor for correct crypto configurations.
- Monitor logs, processes running, and other workload settings 24/7 for indicators of compromise (IoCs) and take immediate action when incidents happen.

Additional resources

- The Truths and Lies of IoT Security
- The Managed Security Services Provider Survival Guide
- There's Help for CISOs Overwhelmed By Security Threats
- True Network Security Depends On More Than Perimeter Defenses

About Masergy

Masergy is the software-defined network and cloud platform for the digital enterprise. Recognized as the pioneer in software-defined networking, Masergy enables unrivaled application performance across the network and the cloud with Managed SD-WAN, UCaaS, CCaaS, and Managed Security solutions. Industry-leading SLAs coupled with an unparalleled customer experience enable global enterprises to achieve business outcomes with certainty.