THE TOP FIVE MYTHS OF HYBRID CLOUD SECURITY

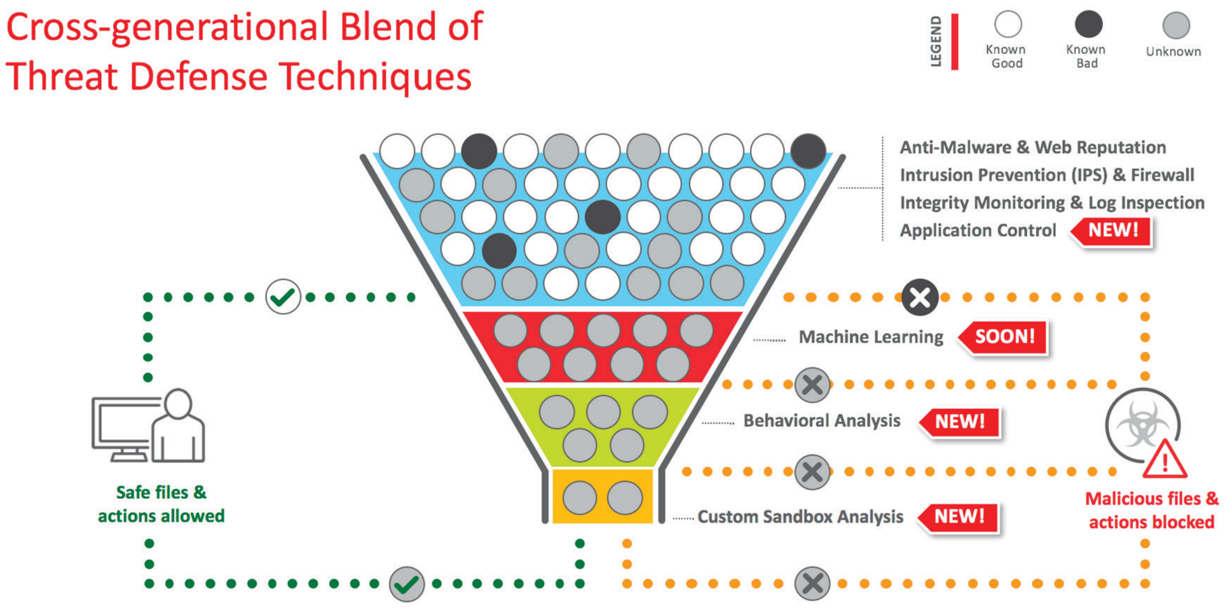
Hybrid cloud security is a hot topic, especially with the massive growth of public cloud providers like Amazon Web Services (AWS), Microsoft® AzureTM and Google Cloud. With the emergence of the hybrid cloud, where workloads are deployed across physical, virtual, and cloud, security professionals are constantly being challenged to evolve their security practices to adapt to this new architecture.

Let's look at the *top five* myths surrounding hybrid cloud security:

MYTH #1: YOU CAN SOLVE SERVER SECURITY WITH ONE TECHNIQUE

While individual security techniques, like application control, can be effective at defending specific types of threats, there is no silver bullet. There is no single technique today that can deal with all of the threats to a server, be it network, file, system, or users. A layered defense is the best defense against modern threats to servers.

Trend Micro Hybrid Cloud Security, powered by XGenTM, takes a blended approach. It combines multiple cross-generational threat defense techniques for protecting hybrid environments. When one technique isn't effective against a given threat, another will step in to eliminate the threat.


Cross-generational Blend of Threat Defense Techniques
LEGEND
Known Good
Known Bad
Unknown
Anti-Malware & Web Reputation
Intrusion Prevention (IPS) & Firewall
Integrity Monitoring & Log Inspection
Application Control
NEW!
Machine Learning
SOON!
Behavioral Analysis
NEW!
Custom Sandbox Analysis
NEW!
Safe files & actions allowed
Malicious files & actions blocked

MYTH #2: YOU CAN'T MANAGE THE HYBRID CLOUD WITH SOLUTIONS FOR THE DATA CENTER

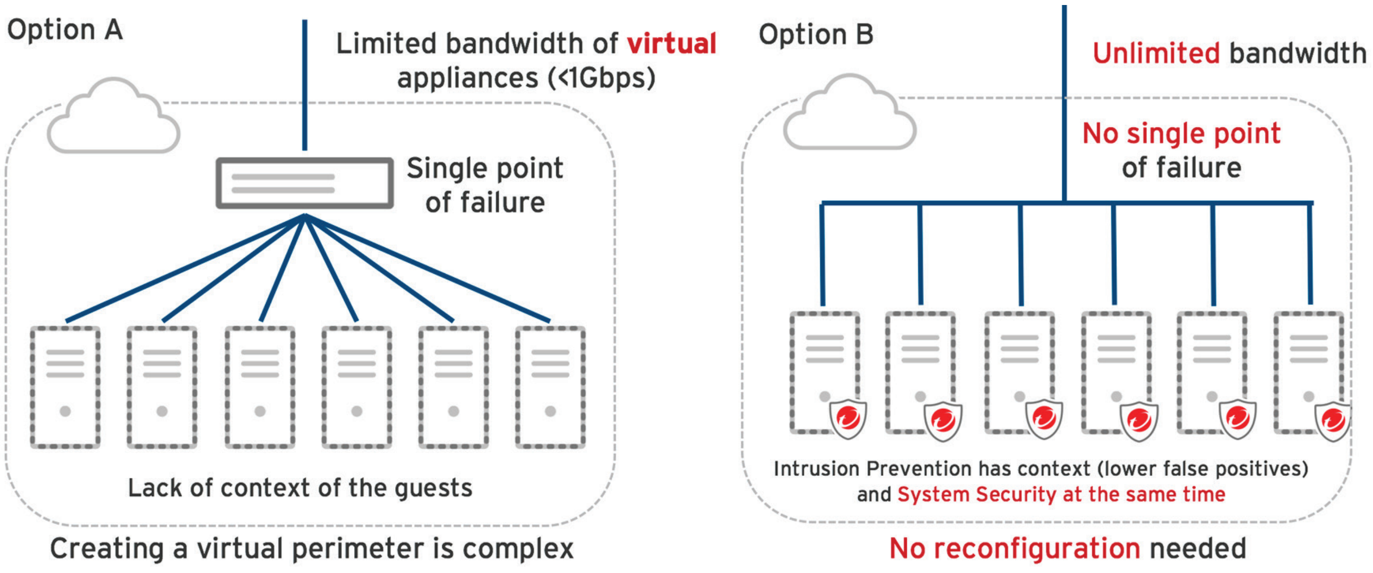
A common misconception is that the tools designed for physical and virtual data centers cannot be used in the cloud. While that is partially true, especially for physical network appliances, some software solutions have been adapted to fit the cloud.

Hybrid Cloud Security, powered by XGenTM, makes the most of hybrid environments by applying the same policies and techniques across environments. With central visibility and control you can effectively manage the hybrid cloud as ONE ENVIRONMENT.

MYTH #3: I SHOULD ALWAYS RELY ON A PERIMITER DEFENSE

If you take a data center mentality into the cloud, you may be in for a shock. Most cloud service providers, like AWS, do not support physical network security devices at the edge. While virtual perimeter solutions are possible, they can be bandwidth limiting and complex to implement. Instead, consider a distributed security posture.

Hybrid Cloud Security, powered by XGenTM, puts firewall, intrusion prevention, and web application protection at the perimeter of each cloud workload for a high performance and context sensitive defense.


Option A
Limited bandwidth of virtual appliances (<1Gbps)
Single point of failure
Lack of context of the guests
Creating a virtual perimeter is complex
Option B
Unlimited bandwidth
No single point of failure
Intrusion Prevention has context (lower false positives) and System Security at the same time
No reconfiguration needed

MYTH #4: I SHOULDN'T TRUST THE CLOUD SERVICE PROVIDER

When you outsource parts of your IT to another provider, the question of trust always comes up. Modern cloud service providers are structured to provide the highest protection for your assets in the cloud. They use separation of duties, logical and physical access, and policies and procedures to create a defensive blanket around what you put in the cloud. In most cases this is far superior to the safeguards in place at an average organization. The main threat model is, was, and always will be external threat actors trying to compromise your servers.

MYTH #5: CLOUD IS THE HARDEST PART OF HYBRID CLOUD SECURITY

From a security perspective, the cloud can often be much easier. You essentially outsource large parts of your security responsibility (physical, hardware shredding, background checks, hypervisor patching and much more). The cloud is often the easiest part of hybrid cloud security. Most providers operate on the shared responsibility model, where they are responsible FOR the cloud while you are responsible for what you put IN the cloud. This reduces your overall burden and many are pleasantly surprised how cloud is the easiest part of hybrid cloud security.

To learn more about the Trend Micro XGen™ endpoint security visit **www.trendmicro.com/xgen**

Securing Your Journey to the Cloud